RCMOS - Multidisciplinary Scientific Journal The Knowledge.
ISSN: 2675-9128. São Paulo-SP.

**Year VI, v.1 2026 | Submission: 01/17/2026 | Accepted: 01/19/2026 | Publication: 01/21/2026**

**Twelve Years Became Five: Software-Induced Obsolescence on PCs Following the End of Windows 10 Support and the End of Windows 11 Requirements**

*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

**Abstract:**

The practical durability of personal computers (PCs) has been progressively reduced not only by physical failures, but also by an increasingly relevant phenomenon: *software-induced obsolescence.* This article investigates, with a delimited focus, how the end of support for Windows 10 on October 14, 2025, and the requirement for a security baseline in Windows 11 (e.g., TPM 2.0 and *Secure Boot)* act as triggers for functional obsolescence, shortening the lifespan of equipment that is still physically capable. The methodology combines document analysis (support policies, minimum requirements, and extended update programs), scenario structuring, and a decision matrix for home users and organizations. The impact on cyber risk, total cost of ownership, and environmental externalities is discussed in light of the National Solid Waste Policy (PNRS) and the reverse logistics of electronic waste in Brazil.

Finally, the study engages with recent regulatory movements in the European Union aimed at promoting repair and ecodesign, proposing practical recommendations for extending service life, lifecycle governance, and more sustainable procurement.
**Keywords:** obsolescence; end of support; life cycle; electronic waste; circular economy.

**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 (eg, 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 INTRODUCTION

The term "obsolescence" is often associated with the inevitable physical wear and tear of equipment. However, in the current context of digital platforms, the practical lifespan of a PC It depends on a set of socio-technical layers: operating system, applications, standards of security, driver compatibility , minimum requirements, and the support policy itself. suppliers. In this scenario, computers that remain functional from the point of view of

**Year VI, v.1 2026 | Submission: 01/17/2026 | Accepted: 01/19/2026 | Publication: 01/21/2026**

*Hardware* can become progressively "unsuitable" for safe and productive use for various reasons. predominantly *software,* characterizing *software*- induced “obsolescence” (Poppe et al., 2021). This article concludes the scope in a technically well-defined event with consequences. broad: the end of support for Windows 10 on October 14, 2025 (Microsoft, 2025), combined to meet the security and compatibility requirements of Windows 11 (Microsoft, 2025).

The transition between Windows versions is a recurring event in the history of personal computing, but Recent dynamics introduce an additional element: the consolidation of a safety baseline. (TPM 2.0, *Secure Boot* and UEFI) which may delete part of the installed system, especially equipment older than certain *CPU/ firmware* cycles (Microsoft, 2025). Even where While *workarounds (temporary alternative solutions )* exist , the relevant discussion for durability is whether... These alternatives preserve safety, performance, compliance, and support within a realistic timeframe.

The relevance of the topic goes beyond technology. The use of unsupported *software* is... frequently cited by cybersecurity agencies as a high-risk practice, as it increases exposure to vulnerabilities and reduced incident response capacity (Cybersecurity and Infrastructure Security Agency, 2025a, 2025b). In parallel, the pressure to upgrade may accelerate The generation of electronic waste, whose global trend remains upward, with gaps between documented generation and recycling (International Telecommunication Union; UNITAR, 2024). In Brazil, the PNRS (National Solid Waste Policy) and specific regulations for reverse logistics of electronic waste establish duties. and instruments to reduce impacts, but the operational challenge remains significant (Brazil, 2010; 2020; 2022).

Given this scenario, this study takes the Windows 10/Windows 11 case as a specific example. empirical to examine how support decisions and technical upgrade parameters reconfigure, In practice, this refers to the durability of PCs that are still physically operational. The investigation starts from the conceptual distinction between *software*- induced obsolescence and obsolescence. hardware material , seeking to clearly define what, in this process, results from natural aging of components and that which results from changes in *software layers,* in Minimum requirements and supplier policies. Next, the closing milestone is described. Windows 10 support and the alternatives available to users and organizations, including options such as extended update programs and continuity strategies that, in practice, They are usually mobilized to reduce risks.

Next, the Windows 11 requirements are mapped out, with emphasis on the criteria. related to safety and compatibility — especially those that condition the update to certain *firmware* and protection bases (such as TPM, Secure Boot and UEFI) — for to understand to what extent such requirements function as technical and institutional barriers to maintaining the use of older equipment. Based on this analysis, the work proposes to

RCMOS – Multidisciplinary Scientific Journal The Knowledge.
ISSN: 2675-9128. São Paulo-SP.

**Year VI, v.1 2026 | Submission: 01/17/2026 | Accepted: 01/19/2026 | Publication: 01/21/2026**

construction of comparable scenarios and a decision matrix capable of guiding choices accordingly.
distinct profiles (home users, small organizations, and corporate environments), considering
security risk, total cost of ownership, expected performance, compliance, and time horizon
Realistic support. Finally, it discusses how the acceleration of replacements may impact generation.
of electronic waste and the pressure on disposal and recycling chains, articulating
the topic relates to the applicable regulatory instruments in Brazil, with emphasis on reverse logistics and for
the mechanisms foreseen in the waste policy that seek to mitigate impacts and expand the destination of waste.
environmentally sound.

## 2 METHODOLOGY

This study adopts a qualitative approach, complemented by a component.
structured decision support, in order to interpret how support policies and requirements of
Compatibility factors act as mechanisms for *software*- induced obsolescence in the case of Windows.
10/Windows 11. The methodology was organized into three main areas. Firstly,
A documentary analysis of official and technical sources related to the purpose of supporting the project was carried out.
Windows 10, the requirements and specifications of Windows 11, and the possibility of adopting...
Extended Security Updates (ESU) as an alternative for temporary continuity. Also
Public guidelines were included that address the risk associated with the use of unsupported *software* .
especially those from cybersecurity organizations that guide best practices
Mitigation and management of vulnerabilities. To support the environmental and regulatory discussion, the following were...
considering the Brazilian framework of the National Solid Waste Policy (PNRS) and its decrees
related issues, in addition to recent European standards that address durability, repairability and
Circularity in electronic products.

Next, based on the documentary evidence and the most important technical constraints...
Given the recurring issues, four typical decision scenarios were constructed, combining user profiles and
compatibility restrictions. These scenarios cover everything from the home user with
equipment compatible with Windows 11, even in situations where the PC does not meet the requirements of
security, CPU or *firmware;* also includes organizations with heterogeneous computing infrastructure and
formal security and compliance obligations; and, finally, organizations that adopt strategies of
Circular economy, prioritizing reuse, refurbishment, reverse logistics, and sustainable purchasing.
as institutional guidelines. The purpose of the scenarios is to represent plausible conditions and
comparable, allowing one to observe how the alternatives for upgrading, migrating, and extended support differ.
Park renovation or improvement produces different results depending on the context.

Based on these scenarios, a decision matrix was developed based on criteria that
They reflect the main *trade-offs* (choices involving gains and losses) of the problem:

**Year VI, v.1 2026 | Submission: 01/17/2026 | Accepted: 01/19/2026 | Publication: 01/21/2026**

safety, total cost of ownership (TCO), operational continuity, environmental impact,
The complexity of implementation and adherence to support. The matrix does not seek to establish a definitive answer.
unique and universal, but to make explicit the possible choices and their consequences, providing a
an instrument to ensure that the decision is technically justified and consistent with the needs of each
profile. Finally, important limitations are acknowledged: the study does not perform empirical measurements of
Performance in specific PC models, nor does it quantitatively estimate emissions or impacts.
environmental factors per unit. The focus is on support mechanisms and requirements and their
decisional implications, so that, especially in organizational environments, it is recommended
To complement the analysis, include an inventory of the installed equipment and a characterization of...
usage profile and a proprietary risk assessment.

## 3. **THEORETICAL FRAMEWORK**

The literature on obsolescence describes how the loss of utility of a good can occur.
through different mechanisms. There is, for example, material obsolescence, related to failures and wear and tear.
physical, and forms of functional and psychological obsolescence, associated, respectively, with the moment
where the product ceases to meet practical needs or the desire for novelty and replacement.
(Sierra-Fontalvo et al., 2023). In the contemporary context of digital platforms, however, the
The functional dimension tends to gain centrality: the "real" lifespan of a PC depends on layers.
socio-technical aspects such as operating system, drivers, application compatibility, minimum standards of
safety and, above all, the supplier's support policy. This means that a piece of equipment may
to remain physically operational and yet become progressively unsuitable for use.
Safe and productive for reasons primarily related to the software.

This finding is directly connected to the concept of software-induced obsolescence.
Poppe et al. discuss *software* obsolescence as a process in which utility degrades not
not due to a physical defect, but due to transformations in the *software* lifecycle and the dependencies that the
surround, distinguishing even between direct and indirect effects (Poppe et al., 2021). In practice, this produces
a compression of the period in which the equipment remains "suitable" for real tasks: even
that the *hardware* remains capable of performing common tasks, the user experience and the level
Acceptable security standards can worsen due to lack of patches, incompatibilities, and changes in...
ecosystem or raising minimum requirements. This compression is particularly sensitive when
“Security” ceases to be a desirable improvement and becomes a minimum requirement for access to
Services, authentication, and network operation.

An important theoretical element in this transition is the consolidation of baselines of

RCMOS – Multidisciplinary Scientific Journal The Knowledge.
ISSN: 2675-9128. São Paulo-SP.

**Year VI, v.1 2026 | Submission: 01/17/2026 | Accepted: 01/19/2026 | Publication: 01/21/2026**

Security as a compatibility criterion. In the case of Windows 11, the requirement for TPM 2.0 and UEFI firmware with Secure Boot capability explicitly sets a goal: raise the minimum bar. boot integrity and credential protection to enable security features. (Microsoft, 2025). This move, while justified from a technical standpoint, also It produces a structuring effect on practical durability: the continuity of supported use becomes depend on platform features that cannot be added or enabled in part of the existing park, even when the equipment performs everyday tasks. Thus, the Software-induced obsolescence emerges not only from the "end of support," but from the interaction between Support policy, security requirements, and ecosystem dependency.

Beyond the technical and conceptual aspects, the discussion is linked to an environmental dimension and regulatory. The acceleration of replacements due to *software* reasons tends to put pressure on the generation of Electronic waste. The Global *E-waste* Monitor 2024 (ITU/UNITAR) records global volumes. records of *e-waste* (discarded or obsolete electronic equipment) and highlights that the Formal, documented recycling is not keeping pace with the rate of growth, with projections of worsening until 2030 (International Telecommunication Union; UNITAR, 2024). In Brazil, this The debate is based on the National Solid Waste Policy, which establishes responsibility. shared by the product life cycle (Brazil, 2010), in addition to diplomas that operationalize Instruments for reverse logistics for electronic waste and regulations under the PNRS (Brazil, 2020; 2022).

At the European level, recent regulations reinforce the agenda for extending service life: the Directive Regulation (EU) 2024/1799 promotes common rules to encourage repair, and Regulation (EU) 2024/1781 creates a framework for ecodesign requirements focused on sustainability and circularity (European Union, 2024a; 2024b). Although the legal regimes are not directly equivalent, these References help contextualize a regulatory trend: reducing premature disposal requires Align incentives, market design, and circularity instruments, and not just transfer them to... The user is responsible for individual exchange decisions.

### 3.1 Support cycle, vulnerabilities and cyber risk

The relationship between the support cycle and cyber risk is crucial to explaining why... Software-induced obsolescence can shorten the practical lifespan of a PC. When a system The operational system is entering end-of-support phase; it will no longer receive regular patches and updates. security, altering the risk balance: vulnerabilities discovered after this milestone tend to remaining without official correction, increasing the likelihood of successful exploitation in Connected environments (Microsoft, 2025; Government of the United Kingdom (GOV.UK), [n.d.]). A Microsoft itself characterizes the end of Windows 10 support as the cessation of updates. Security, software updates, and technical support, even while the system continues to function.

**Year VI, v.1 2026 | Submission: 01/17/2026 | Accepted: 01/19/2026 | Publication: 01/21/2026**

(Microsoft, 2025).

Public cybersecurity guidelines reinforce this reasoning at the operational level: a CISA recommends keeping software up to date and replacing end-of-life hardware or software. precisely because products without support reduce prevention and response capabilities and increase the risk. Exposure to attackers (Cybersecurity & Infrastructure Security Agency (CISA), 2026). This Guidance gains importance in organizational contexts, where the risk is not only technical, but also... Operational and governance: outdated systems tend to require compensatory controls. Segmentation, access restrictions, and additional risk management effort—costs that are not always... These factors appear in the visible price of the equipment, but they directly impact the total cost of ownership. and the migration decision (Joint Task Force; National Institute of Standards and Technology (NIST) 2020; Government of the United Kingdom (GOV.UK), [sd]).

In summary, the support cycle operates as a trigger that reclassifies a computer from "Operating" becomes "operating with increasing risk." Practical durability, therefore, does not end. not only when the *hardware* fails, but when the usage environment demands a minimum level of security and compatibility that an unsupported system can no longer guarantee. This perspective provides a basis for interpreting the Windows 10/Windows 11 transition not simply as a swap of... version, but as an observable case where support, security requirements and dependency of The ecosystem directly influences the acceptable usage time of PCs.

## 4. Results and discussion: "From support to disposal: how to implement update and security policies" They shorten the lifespan of PCs.

Analyzing the Windows 10/Windows 11 case allows us to explain, in a very concrete way, Why do upgrade and security policies shorten the lifespan of PCs? The starting point is... to recognize that the actual lifespan of a computer doesn't depend solely on whether the *hardware* remains ... physically operational, but it remains suitable for use in a connected environment, with manageable risk (National Cyber Security Center (NCSC), [sd]; Government of the United Kingdom (GOV.UK), [n.d.]). In this sense, the end of support for Windows 10 on October 14th. 2025 constitutes a decisive milestone (Microsoft, 2025): from then on, the system can continue to initiate and running programs, but it stops receiving regular security updates and loses support. official technical (Microsoft, 2025; Government of the United Kingdom (GOV.UK), [n.d.]). This This distinction underpins the article's central argument: "functioning" is not synonymous with "remaining." "adequate." For home users, inadequacy tends to appear first as an increase in Exposure to threats and, gradually, incompatibilities and degradation in the ecosystem. (National Cyber Security Center (NCSC), [sd]; Government of the United Kingdom (GOV.UK),

RCMOS - Multidisciplinary Scientific Journal The Knowledge.
ISSN: 2675-9128. São Paulo-SP.

**Year VI, v.1 2026 | Submission: 01/17/2026 | Accepted: 01/19/2026 | Publication: 01/21/2026**

[sd]). For organizations, the problem is exacerbated because operating systems without support can lead to conflicts.
with internal policies, audit requirements and compliance commitments, increasing costs.
Indirect risk mitigation and management methods (Joint Task Force; National Institute of Standards)
and Technology (NIST), 2020; Internet Security, Inc. (CIS®), 2024; NHS England, 2023).

The attempt to "buy time" through Extended Security Updates (Extended)
Security Updates) clearly illustrates the socio-technical nature of this shortening. ESU can reduce risk.
during migration (Microsoft, 2025c; Microsoft, 2025d), but should be read as a bridge, not as
long-term durability solution: usually has a limited lifespan, not necessarily delivering results.
new features and does not replace full ecosystem support (Microsoft, 2025d; Microsoft,
2025e). In practical terms, ESU tends to postpone software-induced obsolescence, without
eliminate it; and, in certain contexts, shift part of the cost to temporary access to maintenance of
security (Microsoft, 2025e). Therefore, even when a transitional strategy is available, it
It does not interrupt the shortening mechanism — it merely reorganizes the decision calendar.
(Microsoft, 2025d; Government of the United Kingdom (GOV.UK), [n.d.]).

The second component is the role of Windows 11 requirements in generating obsolescence.
due to incompatibility. The requirement for a security baseline, such as UEFI with Secure Boot.
and TPM 2.0 (Microsoft, 2025b), can be understood through two lenses that are not mutually exclusive: by one
On the one hand, raising the minimum threshold can reduce the attack surface and enable modern defenses; on the other hand
On the other hand, a portion of the installed devices fail to meet the requirements, creating pressure for early
replacement. It is precisely this coexistence that makes the phenomenon relevant:
The security policy, while strengthening the system for those who are able to migrate,
This can block the migration of still-functional machines. The net result, then, is not just "the
"Windows 11 is more secure," but the ability to maintain secure and supported use is now up to...
It depends on the platform. For equipment without TPM 2.0/Secure Boot (or without compatible CPUs),
The "migrate" option may be unavailable, and you may remain on Windows 10 after support ends.
This implies accepting an increasing risk. (Microsoft, 2025b)

This process intensifies when security ceases to be merely an "improvement" and becomes a requirement
for use. As banks, public services, browsers, and applications raise...
With minimum standards and upgrade requirements, users may reach a "point of no return," in
Simple tasks—such as authentication, accessing services, and secure browsing—become more vulnerable.
or degraded in unsupported systems (Government of the United Kingdom (GOV.UK), [n.d.];
National Cyber Security Center (NCSC), [sd]; Internet Security, Inc. (CIS®), 2024).

Therefore, cybersecurity guidelines explicitly recommend keeping updates and
replace end-of-life software/hardware (Cybersecurity and Infrastructure Security Agency
(CISA), 2025; National Cyber Security Center (NCSC), [sd]; Internet Security, Inc. (CIS®), 2024).

RCMOS - Multidisciplinary Scientific Journal The Knowledge.
ISSN: 2675-9128. São Paulo-SP.

**Year VI, v.1 2026 | Submission: 01/17/2026 | Accepted: 01/19/2026 | Publication: 01/21/2026**

In organizational environments, there is reputational risk and the possibility of incidents involving operational impact (Joint Task Force; National Institute of Standards and Technology (NIST), 2020).

Thus, the shortening does not occur due to a single isolated technical decision, but through interaction. between the end of support, a new security baseline, and ecosystem dependency, which pushes individuals and institutions are forced to migrate within time windows shorter than the physical durability of the environment. the equipment would allow (Google, [n.d.]; Mozilla, [n.d.]).

The discussion, however, is not limited to technology: it reveals economic *trade-offs* and environmental factors. In the total cost of ownership, the domestic user usually perceives primarily the The price of a new computer is high, but for organizations, the hidden costs can be even greater. Inventory, testing, re-approval, training, peripheral adaptation, and risk management—and it is In this context, solutions like ESU can be justified as a transition to migration. staggered (Microsoft, 2025c). In parallel, when *software* change induces replacement. As anticipated, pressure is growing on the generation of electronic waste, as acknowledged in reports. international (International Telecommunication Union; UNITAR, 2024). In Brazil, the PNRS It establishes guidelines and shared responsibility (Brazil, 2010), and there are specific standards. for reverse logistics of household electronic waste (Brazil, 2020) and Decree 10.936/2022 It reinforces implementation instruments (Brazil, 2022), but effectiveness depends on infrastructure and operationalization; therefore, environmental mitigation does not automatically result from the “technological decision.” correct”, but rather of coupled policies and practices, such as reuse, reconditioning and proper disposal. suitable.

Finally, the European debate on repair and *ecodesign* helps to frame the topic as something greater than individual choices. Recent instruments, such as Directive (EU) 2024/1799 (repair) and Regulation (EU) 2024/1781 *(ecodesign)* reinforce that durability can be an objective of public policy and market design (European Union, 2024a, 2024b). Even without transposition Automatically applicable to Brazil, the convergence is clear: if the practical lifespan is shortened by support decisions, safety and compatibility, therefore, extending durability also requires structural solutions, of Governance, regulation, sustainable procurement, and effective circularity mechanisms.

### 4.1 Scenarios: practical decision-making for users and organizations

After demonstrating, throughout the theoretical framework and discussions, that practical durability The timeline for PCs is shortened by the interaction between end of support, raising the security baseline, and... Given the ecosystem's dependence, it becomes necessary to translate this diagnosis into concrete choices. In In other words, if the problem isn't just "switching versions," but managing risk, compatibility, indirect costs and environmental impacts in increasingly shorter time windows,

RCMOS – Multidisciplinary Scientific Journal The Knowledge.
ISSN: 2675-9128. São Paulo-SP.

**Year VI, v.1 2026 | Submission: 01/17/2026 | Accepted: 01/19/2026 | Publication: 01/21/2026**

Therefore, the analysis needs to move from an explanatory level to a decision-making level. That's why the following section...
organizes the Windows 10/Windows 11 case into typical scenarios for users and organizations, reflecting
compatibility restrictions and varying degrees of safety and compliance requirements; then,
It consolidates these alternatives into a qualitative matrix of *trade-offs,* making explicit the...
relative consequences of each strategy in terms of security, TCO, environmental impact, and complexity.
implementation.

C1 — User with a Windows 11 compatible PC. The decision tends to be migration, with caution.
a backup, driver verification, and licensing costs (when applicable). The critical point is planning the
Migration before the degradation of ecosystem support.

C2 — User with incompatible PC. There are three main routes: (a) acquire new equipment; (b)
Remain on Windows 10 with mitigation (ideally ESU when applicable) (Microsoft, 2025);
(c) migrate to another supported operating system (e.g., Linux distributions), considering
learning curve and *software compatibility*. Route (b) is viable only as a transition and
requires caution; route (a) has cost and environmental impact; route (c) can extend service life, but
It depends on the usage profile.

C3 — Organization with a heterogeneous fleet. Here, the migration cost involves inventory, testing,
compatibility, internal/outsourced support, and timeline. The general recommendation is to “update and
Replacing EOL is consistent with security guidelines (Cybersecurity and Infrastructure).
Security Agency, 2025), but an organization can adopt tiered strategies, maintaining
temporarily relocating a subset to ESU and repurposing older equipment for offline use.
controlled laboratories or reconditioning programs.

C4 — Organization with a circular strategy. The challenge is to reconcile safety and extended lifespan.
Studies on ICT circulation in organizations indicate contractual and incentive barriers, in addition to
access to refurbished parts and equipment (Mc-Mahon; Mugge; Hultink, 2024). To overcome
To avoid barriers, it is recommended to integrate circularity and maintenance requirements into contracts, preventing them from...
The only "solution" may be to renew the fleet due to a lack of support.

### 4.2 Decision matrix and trade-offs

Table 1 below presents a qualitative decision matrix (scale).
Low/Medium/High), useful for comparing typical strategies. Results vary depending on context.
But the structure makes the *trade-offs* explicit.

**Table** 1: Decision matrix for post-end-of-support strategies for Windows 10.

| Strategy | Security | TCO | Impact Environmental | Complexity |
|---|---|---|---|---|

RCMOS – Multidisciplinary Scientific Journal The Knowledge.
ISSN: 2675-9128. São Paulo-SP.

**Year VI, v.1 2026 | Submission: 01/17/2026 | Accepted: 01/19/2026 | Publication: 01/21/2026**

| | | | | |
|---|---|---|---|---|
| Migrate to Windows 11 on a compatible computer. | HIGH | AVERAGE | LOW/ AVERAGE | AVERAGE |
| Buy a new computer | HIGH | HIGH | HIGH | LOW/MEDIUM |
| Maintain Windows 10 with ESU (bridge) | MEDIUM/HIGH | AVERAGE | LOW | AVERAGE |
| Keep Windows 10 unsupported after 10/14/25 | LOW | LOW (SHORT TERM) | LOW (SHORT TERM) | LOW |
| Migrating to Linux | MEDIUM/HIGH | LOW/ AVERAGE | LOW | AVERAGE/ HIGH |

**Source:** Author's own work

From a strictly security standpoint, the "unsupported Windows 10" alternative is the more critical and generally not recommended, aligning with warnings about the risk associated with EOL *software* . (Cybersecurity and Infrastructure Security Agency, 2025). From an environmental point of view, the Replacing equipment tends to be the worst option when done prematurely, as it anticipates... Disposal and demand for new manufacturing.

In organizational settings, this type of transition rarely occurs as a "project." "Simple technical" equipment. In practice, it is common for an organization to have a set of equipment. heterogeneous, with machines of different ages and usage profiles, in addition to legacy applications and specific peripherals (printers, scanners, signature modules, proprietary systems) whose Compatibility doesn't always keep pace with updates. Often, migration is... conditioned by operational windows (avoiding critical periods), by approval processes and by contractual dependencies with *software* and support providers. In this context, the decision usually to be sliced: critical and compatible assets are migrated first, a subset is kept in transitional regime (with offsetting controls and, where applicable, extended support), and Older equipment is being repurposed for lower-exposure functions or environments. controlled, until planned replacement is possible.

## 5. Conclusion (or Final Considerations)

This article argues that the practical durability of computers can be reduced in a way... significant through software-induced mechanisms , especially when support policies and Safety requirements establish a compatibility threshold for equipment in use. It cannot overcome this. The Windows 10/Windows 11 case is exemplary because it combines a a well-defined timeframe — the end of Windows 10 support on October 14, 2025 — with Consolidating a security baseline in Windows 11, based on requirements such as TPM.

RCMOS - Multidisciplinary Scientific Journal The Knowledge.
ISSN: 2675-9128. São Paulo-SP.

**Year VI, v.1 2026 | Submission: 01/17/2026 | Accepted: 01/19/2026 | Publication: 01/21/2026**

2.0, Secure Boot, and UEFI, which act as eligibility filters and may block the update in Equipment that is still functional. The result is a shortening of its practical lifespan: computers those that remain physically operational now face increasing risk to remaining on a system without regular updates while migrating to the supported version This may be rendered unfeasible by platform limitations.

The analysis also showed that there is no single solution applicable to all contexts. When the equipment is compatible, migrating to Windows 11 tends to be the most viable option. Consistent from the point of view of continuity and safety. When there is no compatibility, Transition strategies become relevant, especially the use of Security Updates. Extended Urban Mobility (ESU), which can reduce risk in the short term and allow for phased migration, but should to be understood as a bridge, and not as a lasting extension of the life cycle. In some scenarios, Migrating to supported alternative operating systems can extend the practical lifespan, since that is compatible with the usage profile and *software needs;* whereas replacing While this equipment solves the support and compatibility problem, it tends to increase costs and may... intensifies environmental impacts when it occurs prematurely, anticipating disposal and increasing the pressure on the waste chain.

At this point, the environmental and regulatory dimension ceases to be peripheral and becomes an integral part of the overall picture. The rationality of the decision itself. The PNRS (National Solid Waste Policy) structures principles and instruments aimed at prevention, Reducing, reusing, and treating waste, establishing shared responsibility. while specific regulations govern the mandatory reverse logistics for consumer electronics. domestic and reinforce implementation instruments. This implies that technological strategies of Migration and park renovation need to be coupled with formal flows of reuse and reconditioning. and proper disposal, otherwise the security "solution" could result in increased *e-waste.* In parallel, recent initiatives in the European Union — focused on repair and ecodesign — reinforce extending useful life is also a public policy and market design goal, and not It's simply an individual choice for the user.

As a practical implication, the study suggests that decisions made by users and organizations tend to... They become better when they stop being reactive and start being planned. For home users, This means checking compatibility beforehand and avoiding prolonged stays in Unsupported systems; when migration is not feasible, use transitional alternatives such as ESU. when applicable or migrate to supported systems, in addition to reducing exposure in unavoidable uses. (for example, avoid sensitive tasks in unsupported environments and restrict usage to specific contexts) (controlled). For organizations, the recommendation is to treat end-of-life *software* as a material risk. governance, starting with inventory and classification by criticality, adopting hybrid strategies. where critical assets migrate first and the ESU, when used, has a clear exit plan, in addition

**Year VI, v.1 2026 | Submission: 01/17/2026 | Accepted: 01/19/2026 | Publication: 01/21/2026**

to incorporate circularity clauses in ICT contracts (maintenance, replacement of parts, reconditioning, repurchase and proper disposal), given that contractual and other barriers Incentives are important to enable circularity in practice. In all cases, the destination Environmentally sound practices should be treated as part of the decision-making process, adhering to established channels. Formal and auditable, aligned with the PNRS (National Solid Waste Policy) and its regulations, and with risk management principles. Recommended by public cybersecurity guidelines.

As a contribution, this study proposes a replicable framework for future analyses: observe Support milestones and safety requirements as central variables of obsolescence induced by software, linking them to total cost of ownership and environmental impacts. Future research may to quantify emissions avoided by life extension strategies, to compare different ecosystems (Windows, Linux, ChromeOS) and empirically evaluate the effectiveness of policies and refurbishment and reverse logistics programs, with field data and actual inventories of domestic and organizational environments.

## REFERENCES

BRAZIL. Decree No. 10,240, of February 12, 2020 (Reverse logistics of electronic products). 2020. Available at: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/d10240.htm. Accessed on: December 3, 2025.

BRAZIL. Decree No. 10,936, of January 12, 2022 (Regulates the PNRS). 2022. Available at: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2022/decreto/d10936.htm. Accessed on: December 6, 2025.

BRAZIL. Law No. 12,305, of August 2, 2010 (National Solid Waste Policy). 2010. Available at: https://www.planalto.gov.br/ccivil_03/_ato2007-2010/2010/lei/l12305.htm. Accessed on: November 17, 2025.

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY (CISA). Bad Practices (StopRansomware). 2026. Available at: https://www.cisa.gov/stopransomware/bad-practices. Accessed on: December 11, 2025.

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY (CISA). Update Business Software. 2026. Available at: https://www.cisa.gov/audiences/small-and-medium- businesses/secure-your-business/update-business-software. Accessed on: December 16, 2025.

EUROPEAN UNION. Directive (EU) 2024/1799 on common rules promoting the repair of goods. 2024. Available at: https://eur-lex.europa.eu/eli/dir/2024/1799/oj/eng. Accessed on: December 20, 2025.

EUROPEAN UNION. Regulation (EU) 2024/1781 establishing a framework for defining ecodesign requirements for sustainable products. 2024. Available at: https://eur-lex.europa.eu/eli/reg/2024/1781/oj/eng . Accessed on: December 21, 2025.

**Year VI, v.1 2026 | Submission: 01/17/2026 | Accepted: 01/19/2026 | Publication: 01/21/2026**

GOOGLE. Chrome browser system requirements. [n.d.]. Available at: https://support.google.com/chrome/a/answer/7100626?hl=en. Accessed on: January 16, 2026.

GOVERNMENT OF THE UNITED KINGDOM (GOV.UK). Obsolete platforms guidance. 2015. Available at: https://assets.publishing.service.gov.uk/media/5a758829e5274a545822c3e7/Obsolete_platforms_guiDance.pdf. Accessed on: January 16, 2026.

INTERNATIONAL TELECOMMUNICATION UNION (ITU); UNITE. The Global E-waste Monitor 2024. 2024. Available at: https://www.itu.int/en/ITU- D/Environment/Documents/Publications/2025/d-gen-e_waste.01-2024-pdf-e.pdf. Accessed on: December 20, 2025.

INTERNET SECURITY, INC. (CIS®). CIS Controls v8.1 Guide (June 2024). 2024. Available at: https://etir.unb.br/wp-content/uploads/2024/10/CIS_Controls__v8.1_Guide__2024_06.pdf. Accessed on: January 16, 2026.

INTERNET SECURITY, INC. (CIS®). CIS Controls v8.1. [n.d.]. Available at: https://www.cisecurity.org/controls/v8-1. Accessed on: January 16, 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. Available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf. Accessed on: January 16, 2026.

MCMAHON, K.; MUGGE, R.; HULTINK, EJ Overcoming barriers to circularity for internal ict management in organizations: A change management approach. Resources, Conservation and Recycling, v. 205, p. 107568, 2024. Available at: https://www.sciencedirect.com/science/article/pii/S0921344924001630. Accessed on: December 20, 2025.

Microsoft. Extended Security Updates (ESU) program for Windows 10. 2025. Available at: https://learn.microsoft.com/en-us/windows/whats-new/extended-security-updates. Accessed on: January 16, 2026.

MICROSOFT. Product Lifecycle FAQ – Extended Security Updates. [sd]. Available at: https://learn.microsoft.com/en-us/lifecycle/faq/extended-security-updates. Accessed on: January 16, 2026.

MICROSOFT. Stay secure with Windows 11, Copilot+ PCs and Windows 365 before support ends for Windows 10. 2025. Available at: https://blogs.windows.com/windowsexperience/2025/06/24/stay-secure-with-windows-11-copilot- pcs-and-windows-365-before-support-ends-for-windows-10/. Accessed on: January 16, 2026.

MICROSOFT. Windows 10 Consumer Extended Security Updates (ESU). 2025. Available at: https://www.microsoft.com/en-us/windows/extended-security-updates. Accessed on: December 21, 2025.

**Year VI, v.1 2026 | Submission: 01/17/2026 | Accepted: 01/19/2026 | Publication: 01/21/2026**

Microsoft. Windows 10 support has ended on October 14, 2025. 2025. Available at: https://support.microsoft.com/en-us/windows/windows-10-support-has-ended-on-october-14-2025-2ca8b313-1946-43d3-b55c-2b95b107f281. Accessed on: December 21, 2025.

MICROSOFT. Windows 11 Specs and System Requirements. 2025. Available at: https://www.microsoft.com/en-us/windows/windows-11-specifications. Accessed on: December 21, 2025.

MOZILLA. What Windows 10 end of support means for Firefox users. [sd]. Available at: https://support.mozilla.org/en-US/kb/firefox-support-windows-10-end-support. Accessed on: January 16, 2026.

NATIONAL CYBER SECURITY CENTER (NCSC). Keeping devices and software up to date. [sd]. Available at: https://www.ncsc.gov.uk/collection/device-security-guidance/managing- deployed-devices/keeping-devices-and-software-up-to-date. Accessed on: January 16, 2026.

NATIONAL CYBER SECURITY CENTRE (NCSC). Obsolete products. [n.d.]. Available at: https://www.ncsc.gov.uk/collection/device-security-guidance/managing-deployed-devices/obsolete-products . Accessed on: January 16, 2026.

NHS ENGLAND. Data Security Standard 8: unsupported systems. 2023. Available at: https://www.dsptoolkit.nhs.uk/News/Attachment/765. Accessed on: January 16, 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): [sn], 2021. Available at: https://researchrepository.ul.ie/bitstreams/2e091cb3-6520-4e3b-a806-eee74d3f9682/download. Accessed on: December 20, 2025.

SIERRA-FONTALVO, L. et al. A deep dive into addressing obsolescence in product design. Heliyon, 2023. Available at: https://www.sciencedirect.com/science/article/pii/S2405844023090643. Accessed on: December 20, 2025.