Machine Translated by Google
NOMOS - Multidisciplinary Scientific Journal
Knowledge. ISSN: 2675-9128. São Paulo-SP.

Year VII, v.2 2026 | Submission: October 8, 2026 | Accepted: October 10, 2026 | Publication: October 13, 2026

**Data resilience in hybrid infrastructures: architecture, protection, recovery, and governance.**

*Data resilience in hybrid infrastructures: architecture, protection, recovery and governance*
Data resilience in hybrid infrastructures: architecture, protection, recovery and governance

**Eduardo Eneas Pereira Nunes**

Bachelor of Science in Computer Science from the São Paulo State University "Júlio de Mesquita Filho" (Unesp), São José do Rio Preto campus; Postgraduate degree (Lato Sensu) in Telecommunications Networks from the Federal University of Minas Gerais; MBA in Project Management from the University of São Paulo (USP), Piracicaba campus; Information Technology Professional.

**SUMMARY**
The continuity of digital services depends less on the abstract existence of a backup than on the proven ability to restore data, applications, and dependencies within limits accepted by the business. This article examines data resilience in hybrid infrastructures, where local, virtualized, and cloud resources form technical and contractual chains that are difficult to observe as a whole. The research problem consists of determining which dimensions allow for the evaluation of a protection architecture beyond the acquisition of products.
A qualitative bibliographic and documentary review was adopted, supported by standards, institutional publications, and scientific literature. The analysis organizes six dimensions: storage architecture, copies and isolation, cyber threat, recovery objectives, hybrid governance, and operational validation. It concludes that resilience is a systemic and measurable property, produced by the coherence between criticality, design, controls, testing, and learning. Contracted capacity without exercised restoration remains only an expectation.
Keywords: data resilience; storage; backup; disaster recovery; hybrid cloud; governance.

**ABSTRACT**
Digital service continuity depends less on the abstract existence of a backup than on the demonstrated ability to restore data, applications and dependencies within business-approved limits. This article examines data resilience in hybrid infrastructures, where on-premises, virtualized and cloud resources form technical and contractual chains that are difficult to observe as a whole. The research problem asks which dimensions make it possible to assess a protection architecture beyond product acquisition.

A qualitative bibliographic and documentary review was conducted using standards, institutional publications and scientific literature. The analysis is organized around six dimensions: storage architecture, copies and isolation, cyber threats, recovery objectives, hybrid governance and operational validation. The study concludes that resilience is a systemic and measurable property created by coherence among criticality, design, controls, testing and learning. Purchased capacity without exercised restoration remains an expectation rather than an operational capability.
Keywords: data resilience; storage; backup; disaster recovery; hybrid cloud; governance.
Keywords: data resilience; storage; backup; disaster recovery; hybrid cloud; governance.

## INTRODUCTION

Digital information occupies a paradoxical position in contemporary organizations. It sustains transactions, logistics, customer relations, research and administrative decisions, but its usefulness

This is an open access article published under the Creative Commons Attribution license, which allows its use.
Distribution and reproduction in any medium, without restrictions, provided the original work is properly cited.

Machine Translated by Google


**Year VII, v.2 2026 | Submission: October 8, 2026 | Accepted: October 10, 2026 | Publication: October 13, 2026**

It depends on an infrastructure that often disappears from view while it's operating.
The interruption makes visible, all at once, dependencies between storage, identity, network, applications and people. The cost doesn't just stem from the loss of files; it includes downtime, Reconstruction, investigation, legal obligations, and erosion of trust.

Cloud expansion increases capacity and flexibility, without eliminating the problem of continuity. Gartner estimated that worldwide end-user spending on public cloud services would increase from US$595.7 billion in 2024 to US$723.4 billion in 2025, a growth of 21.5% (GARTNER, 2024). The same movement distributes data by region, account, provider, and model. Responsibility. Architectural complexity, not a lack of technology, becomes a central source. exhibition.

NIST *(National Institute of Standards and Technology )* Technology) – a United States government agency attached to the Department of Commerce – describes the evolution of storage from block, file, and object services to abstractions. defined by software and cloud access. For Chandramouli and Pinhas (2020), this path This increases management complexity and the likelihood of configuration errors. Observation removes A purely ableist interpretation: more copies or more terabytes do not, in themselves, mean greater Security. Access controls, isolation, encryption, integrity, and restoration need to be integrated. a coherent design.

Given this scenario, the article asks how to assess data resilience in hybrid environments. without reducing it to the purchase of backups. The goal is to build an analytical synthesis that relates Architecture, threat, recovery, governance, and operational evidence. No comparison is intended. suppliers should not report individual professional experiences. The contribution lies in converting Scattered recommendations across criteria that can guide design, auditing, and applied research.

## METHODOLOGY

The research is qualitative, exploratory, and based on a literature and document review. Selected classic scientific publications on cloud computing, redundancy, and systems. distributed, in addition to standards and technical guides produced by NIST, ISO, CISA, ENISA, CIS, IBM and Gartner. The combination allows for bridging the gap between enduring fundamentals and recent market data. and threats.

The conceptual search prioritized the descriptors *data resilience, storage security, backup, disaster. recovery, business continuity, hybrid cloud, ransomware, and recovery objectives.* Inclusion required identifiable authorship, institutional affiliation or recognized academic publication, date and address.

This is an open access article published under the Creative Commons Attribution license, which allows its use.
Distribution and reproduction in any medium, without restrictions, provided the original work is properly cited.

Machine Translated by Google


**Year VII, v.2 2026 | Submission: October 8, 2026 | Accepted: October 10, 2026 | Publication: October 13, 2026**

Persistent or DOI *( Digital* Object Identifier) code

A unique and persistent alphanumeric code used to identify digital documents and files. Contents

Commercials were used only when they presented stated research or market figures.

attributable, but never as sufficient proof of a product's effectiveness.

The corpus was analyzed by categories. The first category includes structure and redundancy; the second deals with protection,

Isolation and immutability; the third covers cyber risk; the fourth examines continuity, RPO, and

RTO; the fifth addresses hybrid cloud and shared responsibility; the sixth discusses testing.

Indicators and learning. Statements were compared across different source types to reduce

dependence on a single institution.

Table 1 summarizes this organization and explains the correspondence between each dimension and the question.

which guides your reading and the predominant sources, making the analytical path verifiable.

Table 1 - Analytical dimensions, guiding questions, and corpus sources

| **Analytical dimension:** | **Question that guides the reading.** | **Main sources mobilized** |
|---|---|---|
| Architecture of storage | How availability is built In layers? | Patterson, Gibson and Katz (1988); Chandramouli and Pinecones (2020) |
| Copies, isolation and integrity | The copy is recoverable and independent. From the production? | Chandramouli and Pine Cones (2020); CIS (2021) |
| Cyber threat | The opponent achieves production and recovery? | ENISA (2024); CISA (2023) |
| Objectives of recovery | RPO and RTO are derived from the analysis of What impact on the business? | Swanson et al. (2010); ISO 22301:2019 |
| Hybrid governance | Who is responsible for classification, Retention and exit? | Mell and Grance (2011); Armbrust et al. (2010); Gartner (2024, 2025) |
| Validation operational | There is evidence of tested restoration. And dated? | CIS (2021); ISO/IEC 27001:2022 |

Source: own elaboration (2025).

The financial figures are presented in current US dollars and maintain the time frame of the source.

Predictions are identified as predictions, not as realized results. The graph reproduces

Values published by Gartner in November 2024. Limitations include the rapid...

Technological evolution, regulatory differences between countries, and the absence of primary data on

specific organizations.

This is an open access article published under the Creative Commons Attribution license, which allows its use.
Distribution and reproduction in any medium, without restrictions, provided the original work is properly cited.

Machine Translated by Google


**Year VII, v.2 2026 | Submission: October 8, 2026 | Accepted: October 10, 2026 | Publication: October 13, 2026**

The tables and figures in this article were created by the author. When reproducing data from a source...
In the primary context, the origin is indicated in the caption itself; when organizing the content discussed in the review,
These are analytical summaries, and the reference values are for illustrative purposes only, with no intention of representing a measurement.
empirical.

The interpretation adopts a socio-technical logic. Controls are evaluated in relation to people,
business processes, contracts, and objectives, avoiding the assumption that the presence of a tool
Demonstrate functionality. Analytical validity stems from traceability of sources and consistency.
between categories, not statistical generalization. Future empirical studies could test the model.
in different sectors and sizes.

## STORAGE ARCHITECTURE AND THE CONSTRUCTION OF AVAILABILITY

Modern availability results from layers, not from a single infallible component. The classic approach
Patterson, Gibson and Katz (1988) showed how record arrangements could combine performance
and fault tolerance through redundancy. The idea remains relevant, but needs to be contextualized:
RAID *(Redundant Array of Independent Disks )*
Protects against certain media defects; does not replace standalone copies or version history.
or recovery after logical impairment.

The transition from directly attached storage to networks, distributed systems,
Hyperconvergence and cloud services have increased scalability options. They have also multiplied plans for...
control, credentials, and interfaces. Chandramouli and Pinhas (2020) recommend that security
Consider authentication, authorization, configuration, media protection, isolation, encryption, and...
Answer. The protected object is no longer just the volume; it includes metadata and mechanisms that make it...
usable volume.

Redundancy and recoverability belong to different categories. Synchronous replicas can maintain
The service fails when a node fails, but it can also propagate exclusions, corruption, or malicious actions.
Versioned copies preserve previous states, although they may remain inaccessible if...
They share credentials or administrative domain with production. A mature architecture.
It combines mechanisms with distinct failure modes.

Table 2 organizes this distinction, relating each mechanism to the flaws it effectively covers.
to the limits it preserves and the role it plays in the recovery of the service.

This is an open access article published under the Creative Commons Attribution license, which allows its use.
Distribution and reproduction in any medium, without restrictions, provided the original work is properly cited.

Machine Translated by Google


**Year VII, v.2 2026 | Submission: October 8, 2026 | Accepted: October 10, 2026 | Publication: October 13, 2026**

Table 2 - Protection mechanisms: covered faults, limits and role in recovery

| **Mechanism** | **Protects against** | **It does not protect against** | **Role in recovery** |
|---|---|---|---|
| RAID and protection media | Disk failure, sector defective | Exclusion logic, corruption, access with valid credential | Maintain the service. available; does not create historical |
| Synchronous replica | Failure of node, controller or site | Immediate spread of exclusion and corruption | It supports the operation; does not offer a point of return |
| Snapshot node same system | Error recent of user or application | Loss of the system that hosts the snapshot | Quick return to short windows |
| Backup versioned in another domain | Exclusion, corruption and loss of site | Privileged credential shared with production | Base of the point historical recovery |
| Immutable copy (WORM) | Change and delete during detention | Data already encrypted before to be copied | Ensures persistence. from the preserved version |
| Offline copy or isolated (air gap) | Attack that reaches the control plan | Larger loss window and slower restoration | Last resource reliable chain |

Source: own elaboration based on Patterson, Gibson and Katz (1988) and Chandramouli and Pinhas (2020).

Figure 1 converts the same reading into a coverage matrix. The incomplete diagonal highlights...

The central argument: no single mechanism accounts for all failure modes, and resilience

This results from a combination of controls with independent failures.

This is an open access article published under the Creative Commons Attribution license, which allows its use.
Distribution and reproduction in any medium, without restrictions, provided the original work is properly cited.

Machine Translated by Google
FOMOS - Multidisciplinary Scientific Journal
Knowledge. ISSN: 2675-9128. São Paulo-SP.

**Year VII, v.2 2026 | Submission: October 8, 2026 | Accepted: October 10, 2026 | Publication: October 13, 2026**

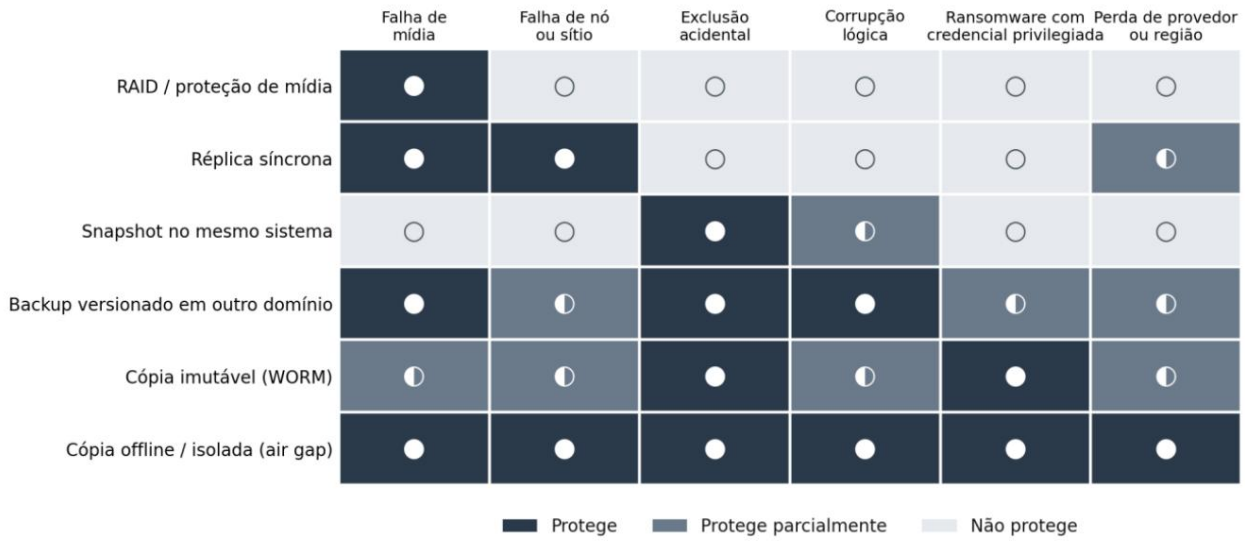



Figure 1 - Coverage matrix between protection mechanisms and failure modes. Source: [Company Name] own (2025).

Another point is granularity. Transactional applications require consistency between banks, queues, files and catalogs; copying each component at disconnected times can produce a set Impossible to restart. Therefore, protection must be based on dependency maps and consistent states. The physical design only acquires meaning when related to the logical sequence of service restoration. Data classification avoids treating everything the same way. Criticality, frequency of change, Legal retention, sensitivity, and cost of recovery guide different policies. A basis Operational data may require low permissible loss, while a historical repository tolerates a larger window. Differentiation has costs and prevents real priorities from dissolving into a uniform policy. Architecture must, ultimately, record its premises. Volume, growth rate, protection window, Bandwidth, dependencies, and responsibilities need to be measurable. Without this inventory, Capacity is limited by past performance and silently fails in the face of growth. Project Resilient refers to a characteristic whose suitability can be recalculated when the environment changes.

## COPIES, ISOLATION AND INTEGRITY

Backup is a preservation process geared towards recovery, not a file repository. Quality depends on coverage, consistency, retention, and the ability to locate versions. Useful. High task completion rates may hide deleted applications and credentials. expired or logically inconsistent copies. The central indicator should approach the result. restorable.

This is an open access article published under the Creative Commons Attribution license, which allows its use.
Distribution and reproduction in any medium, without restrictions, provided the original work is properly cited.

Machine Translated by Google
RGMOS - Multidisciplinary Scientific Journal
Knowledge. ISSN: 2675-9128. São Paulo-SP.

**Year VII, v.2 2026 | Submission: October 8, 2026 | Accepted: October 10, 2026 | Publication: October 13, 2026**

The separation between fault domains is a crucial principle. If production and copies depend on...
Even with the same privileged identities, a compromised credential can affect both. Isolation
Physical, logical, or temporal measures reduce this spread. NIST (2020) includes protection, isolation, and
Guaranteed restoration is among the specific recommendations for storage infrastructure.

Table 3 compares copy composition strategies that are widely referenced in practice.
operational, showing what each arrangement adds and what limit remains after adopting it.

Table 3 - Copywriting strategies: what they reinforce and what they don't solve

| **Strategy** the | **Composition** | **Which reinforces** | **Limit that remains** |
|---|---|---|---|
| 3-2-1 | Three copies, two types of media, one out of place | Media diversity and geographical dispersion | It does not require immutability. nor verification of integrity |
| 3-2-1-1-0 | Add a copy immutable or offline and no errors in verification | Ransomware resistance and evidence of copying readable | Cost and complexity of retention management |
| 4-3-2 | Four copies, three locations, two outside the site | Additional redundancy for regulated environments | It requires orchestration and continuous testing |

Source: own elaboration based on CISA (2023) and CIS (2021).

Immutability adds resistance to change during a defined window, but does not correct retention.
Inadequate encryption does not guarantee that the content will be clean. An immutable copy of data already encrypted by
The attacker preserves the damage. Control needs to be associated with detection, previous versions, and analysis of...
Recovery point. Useful technology becomes dangerous when its label replaces understanding.
of the mechanism.

Cryptography protects confidentiality in transit and at rest, but introduces key dependency.
Unavailable keys render an intact copy unusable; exposed keys invalidate the data.
Part of the protection. Lifecycle management, segregation of duties, rotation and safe recovery.
They should be integrated into the same plan. Backup security includes the security of your access methods.
Integrity requires continuous verification. Hashes and validations detect changes, but only tests...
Reading and restoration processes reveal cataloging, linking, or compatibility issues. A
Automation can increase sampling and frequency, provided that failures result in treatment and not
Only accumulated alerts. Operational evidence must include an assigned person, a deadline, and acceptance criteria.
Retention also has economic and legal dimensions. Holding everything indefinitely increases
cost, surface area, and search complexity; eliminating too early compromises
Recovery and liabilities. Policies must reconcile business needs, legislation, and litigation.

This is an open access article published under the Creative Commons Attribution license, which allows its use.
Distribution and reproduction in any medium, without restrictions, provided the original work is properly cited.

Machine Translated by Google
NOMOS - Multidisciplinary Scientific Journal
Knowledge. ISSN: 2675-9128. São Paulo-SP.

**Year VII, v.2 2026 | Submission: October 8, 2026 | Accepted: October 10, 2026 | Publication: October 13, 2026**

predictable and minimization. The result is a justifiable retention matrix, revised and linked to
data classification.

**Ransomware and Cyber Resilience**

Ransomware has transformed recovery into a strategic security problem. The landscape of
ENISA *( European* Union Agency for Cybersecurity)
Cybersecurity) for 2024 placed threats to availability at the top and ransomware right after.
followed by an analysis of thousands of reported incidents. The data suggests that confidentiality
That's not enough: the organization needs to sustain or rebuild services under pressure and with information.
incomplete.
Figure 2 details this distribution. Threats to availability and ransomware, combined, account for...
Threats account for approximately two-thirds of the incidents analyzed, and data threats occupy the third position.
The profile reinforces the article's interpretation: the majority of the observed volume attacks precisely the capacity.
to operate and to return.

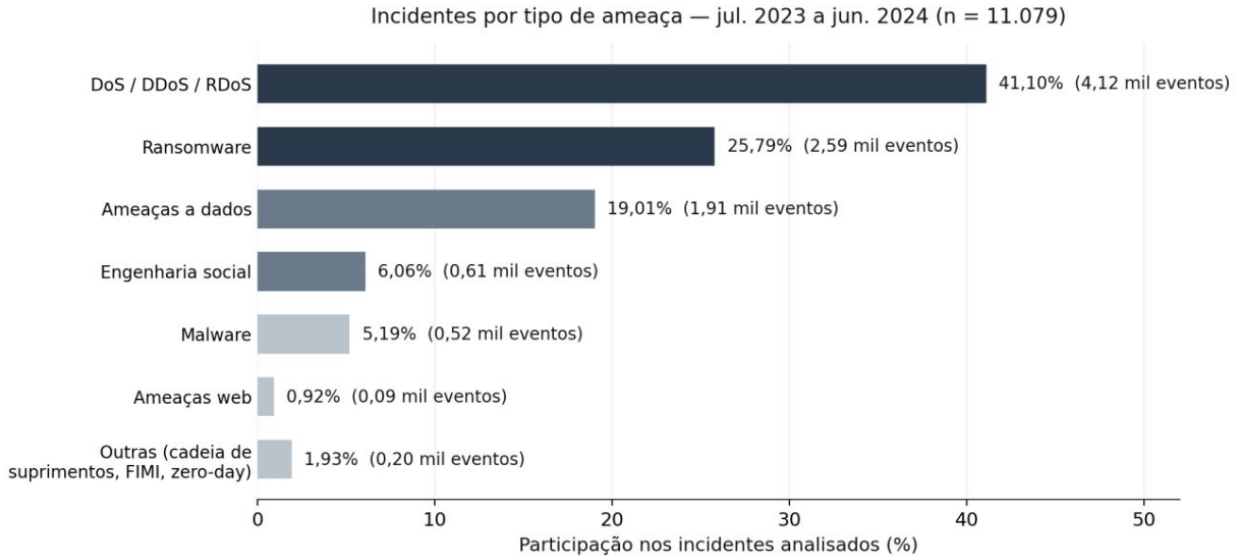



Figure 2 - Distribution of analyzed incidents by threat type, July 2023 to June 2024.
Source: own elaboration with data from ENISA (2024).
Modern attacks target credentials, administrative consoles, hypervisors, and repository security systems.
Copy. The defense cannot assume an intact perimeter. Minimum privilege, strong authentication.
Account segregation, protected administrative pathways, and action logging reduce the chance of
A single access point can dominate the entire chain. The design must take into account the adversary already present.
Table 4 lists the most frequent targets in the recovery chain, the intended effect by
The attacker, priority control, and the evidence that allows one to affirm that control is in operation.

This is an open access article published under the Creative Commons Attribution license, which allows its use.
Distribution and reproduction in any medium, without restrictions, provided the original work is properly cited.

Machine Translated by Google
NOMOS - Multidisciplinary Scientific Journal
Knowledge. ISSN: 2675-9128. São Paulo-SP.

**Year VII, v.2 2026 | Submission: October 8, 2026 | Accepted: October 10, 2026 | Publication: October 13, 2026**

Table 4 - Ransomware targets in the recovery chain and corresponding controls

| **Target in prison** | **Objective of attacker** | **Priority control** | **Expected evidence** |
|---|---|---|---|
| Identity and accounts privileged | To obtain access broad administrative | Privilege minimum, Strong authentication, accounts separated | Account inventory privileged reviewed |
| Console of backup | Reduce retention, to switch off jobs and catalogs | Administrative domain distinct and double approval | Change log retention policy |
| Hypervisor and control plan | Encrypt many single services time | Segregated management network and stock registry | Audit trail with periodic review |
| Repository of copies | Preventing a return to previous states | Immutability, copy isolated and credentials own | Restoration tested at starting from the isolated copy |
| Snapshots and replicas | Eliminate points of recent returns | Keep out of reach from the production account | Verification automatic of existence and age |
| Keys of cryptography | To render unusable full copy | Custody segregated, rotation and copy of recovery | Exercise documented of key recovery |

Source: own elaboration based on CISA (2023), ENISA (2024) and Chandramouli and Pinhas (2020).

CISA *(Cybersecurity and Infrastructure Security Agency,* or Cybersecurity and Infrastructure Security Agency) (Infrastructure) recommends offline, encrypted, and tested backups as part of the response to Ransomware. The word "tested" shifts the focus: storing is not the same as recovering. Exercises They need to verify data, upload sequence, identities, networks, keys, and team capacity.

A successfully restored file does not guarantee that the entire service will be back up and running within the required timeframe. Detection must reach the data plane. Abrupt changes in the modification rate, compression, Account deletions or behavior may indicate an attack before a complete block. However, Strict thresholds produce false positives in legitimate routines. The baseline must be aware of cycles. Closing procedures, analytical loads, and maintenance are used to distinguish anomalies from seasonality.

Recovering from a compromised environment can restart the incident. It is necessary to define a clean area. Trust criteria and validation steps before reconnecting systems. Images, settings and

This is an open access article published under the Creative Commons Attribution license, which allows its use.
Distribution and reproduction in any medium, without restrictions, provided the original work is properly cited.

Machine Translated by Google


**Year VII, v.2 2026 | Submission: October 8, 2026 | Accepted: October 10, 2026 | Publication: October 13, 2026**

Credentials need to be examined; external dependencies, reauthorized. Speed matters.
However, a rushed restoration could extend the total downtime.
Communication is an integral part of resilience. Decisions regarding shutdowns, prioritization, notification, and resumption.
It involves management, legal, security, operations, and business areas. Roles are predefined.
They reduce disputes during the crisis. After the event, the analysis should transform evidence into...
Architectural and procedural corrections, closing the loop between incident and learning.

**RPO, RTO, and Business Continuity**

Two parameters organize the conversation about recovery. The recovery point objective, RPO, expresses
The maximum data loss allowed over time; the recovery time objective, RTO, indicates the timeframe.
desired for restoration. Both are objectives, not automatic characteristics of a
tool. They need to derive from the impact on processes and be confronted with technical capacity.
real.
Swanson et al. (2010) situate contingency planning within the life cycle of systems and
They recommend evaluating operations to determine priorities. Business impact analysis provides
This connection. It identifies essential services, dependencies, effects of disruption, and tolerances.
Without such a foundation, RPO and RTO tend to reflect technical convenience or ambition without budget.
Aggressive objectives have costs. Reducing acceptable loss may require frequent replication, resulting in greater efficiency.
Consistent bandwidth and capture mechanisms. Reducing turnaround time demands
Reserved capacity, automation, and trained teams. The balance is not about choosing between security and...
economics, but specify how much each level costs and what loss it aims to limit.
Table 5 illustrates how the criticality classification translates this negotiation into distinct parameters.
by service class, avoiding uniform policies for unequal needs.

This is an open access article published under the Creative Commons Attribution license, which allows its use.
Distribution and reproduction in any medium, without restrictions, provided the original work is properly cited.

Machine Translated by Google
RCMOS - Multidisciplinary Scientific Journal
Knowledge. ISSN: 2675-9128. São Paulo-SP.

Year VII, v.2 2026 | Submission: October 8, 2026 | Accepted: October 10, 2026 | Publication: October 13, 2026

Table 5 - Criticality classes, reference objectives and associated mechanisms

| Class | Example of service | RPO / RTO of reference | Mechanism predominant | Cost relative |
|---|---|---|---|---|
| Review | Online transaction, service to the customer | Minutes / up to 1 hour | Replication continuous with immutable copy | Very high |
| Essential | ERP, billing, integrations | Up to 1 hour / up to 4 hours | Asynchronous replica and frequent backups | High |
| Important and | Collaboration, internal reports | Up to 12 hours / up to 24 hours | Backup daily versioned | Moderate |
| Of support | Historical repository, cold files | Up to 24 hours / up to 72 hours | Periodic backup with long retention | Low |

Source: own elaboration based on Swanson et al. (2010) and ISO 22301:2019. The intervals are

Illustrative and should be derived from an impact analysis on each organization's business.

Figure 3 represents the trend that underpins this differentiation. As the objectives become

They become more stringent, the cost increases sharply, which explains why uniform requirements

They tend to be abandoned in practice or funded only in discourse.

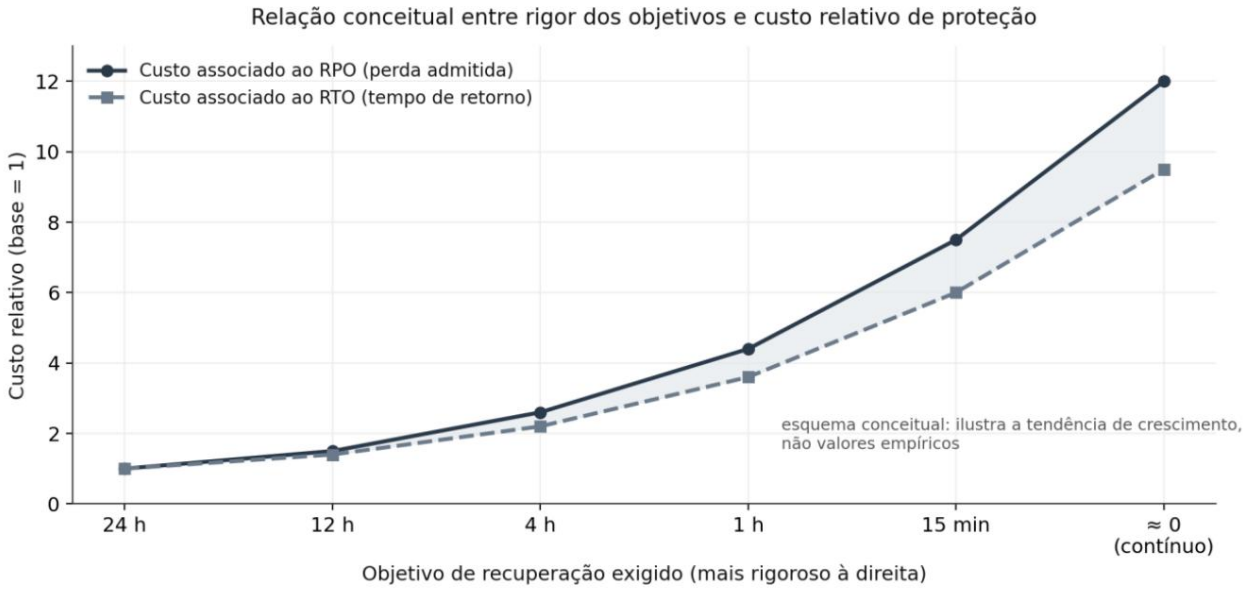



Figure 3 - Conceptual relationship between the rigor of recovery objectives and the relative cost of protection.

Source: own elaboration (2025); conceptual scheme, without empirical values.

Recovery occurs sequentially. Identity, network, name services, databases, and integrations can all be affected.

Precede the application visible to the user. Measuring only the volume restore time underestimates the

This is an open access article published under the Creative Commons Attribution license, which allows its use.
Distribution and reproduction in any medium, without restrictions, provided the original work is properly cited.

Machine Translated by Google


**Year VII, v.2 2026 | Submission: October 8, 2026 | Accepted: October 10, 2026 | Publication: October 13, 2026**

Service duration. Dependency maps and ordered runbooks transform RTO into a plan.
executable files allow you to locate bottlenecks before a crisis occurs.

ISO 22301:2019 addresses continuity as a management system, with policy, analysis, strategy,
Plans, exercises, and improvement. This structure prevents recovery from being an isolated annual event.
Changes in architecture, team, or supplier should trigger a review of the plans. The goal
It remains stable only as long as its premises remain true.

Metrics need to distinguish between intent and evidence. Application coverage, age of the last copy.
Validity, percentage of approved restorations, time observed, and divergence from the objective.
They provide a more honest view. Results should be segmented by criticality; an average
In general, it may be hiding precisely the service that cannot fail.

**Hybrid Cloud, Portability, and Responsibility**

NIST's definition of cloud emphasizes on-demand access to a shared set of resources.
configurable (MELL; GRANCE, 2011). The model shifts part of the operation to the provider, but
It does not automatically transfer classification, retention, identity, and continuity. Responsibilities
They vary by service and contract. Making assumptions about them is a recurring risk.

Table 6 illustrates this variation by service model and shows that classification, testing of
Restoration and portability remain with the customer in all arrangements, even if the operation
underlying change of hands.

This is an open access article published under the Creative Commons Attribution license, which allows its use.
Distribution and reproduction in any medium, without restrictions, provided the original work is properly cited.

Machine Translated by Google
RCMOS - Multidisciplinary Scientific Journal
Knowledge. ISSN: 2675-9128. São Paulo-SP.

Year VII, v.2 2026 | Submission: October 8, 2026 | Accepted: October 10, 2026 | Publication: October 13, 2026

Table 6 - Distribution of responsibilities by service model

| Protective item | Installation local | IaaS | PaaS | SaaS |
|---|---|---|---|---|
| Physical infrastructure Client | | Provider | Provider | Provider |
| Settings of service | Customer | Customer | Shared Provider | |
| Classification of data | Customer | Customer | Customer | Customer |
| Customer Identity and Access | | Customer | Shared Shared | |
| Copy and Retention | Customer | Customer | Shared | It depends. of contract |
| Key management | Customer | Customer or shared | Shared | Provider or optional |
| Client restore test | | Customer | Customer | Customer |
| Portability and customer exit | | Shared Shared | | It depends. of contract |

Source: own elaboration based on Mell and Grance (2011) and Armbrust et al. (2010). Attribution
Effectiveness depends on the contract and the service contracted.

Armbrust et al. (2010) identified elasticity and economies of scale as driving forces of computing.
in the cloud, alongside obstacles such as availability, lock-in, and confidentiality. In
In hybrid environments, these tensions accumulate. Data can circulate between dedicated facilities,
Software as a service and multiple regions, each with different protection mechanisms and
export.

Portability must be tested, not inferred from generic clauses. Formats, APIs, metadata,
Keys and egress rates influence the possibility of recovery or migration. A stored copy
within the same service, it can respond to accidental exclusions, but offers little independence in the face of
widespread unavailability or contract termination. The scenario determines the degree of separation.
necessary.

Sovereignty adds jurisdiction and location to the design. Rules of privacy, access
Governmental and international transfers can limit regions and operators. The Gartner (2025)
He highlighted digital sovereignty as one of the trends shaping the cloud and predicted significant growth.
of specific strategies in multinational companies until 2029. Predictions are not accomplished facts, but
They signal governance pressure.

This is an open access article published under the Creative Commons Attribution license, which allows its use.
Distribution and reproduction in any medium, without restrictions, provided the original work is properly cited.

Machine Translated by Google


**Year VII, v.2 2026 | Submission: October 8, 2026 | Accepted: October 10, 2026 | Publication: October 13, 2026**

Variable costs require financial observability. Storage, requests, retrieval and
Transfers can change the total cost depending on retention and exercises. Optimization that reduces
Copying or testing to save expenses can increase operational exposure. FinOps applied to
Protection should link spending to criticality, coverage, and evidence of recovery.
Contracts complete the architecture. Service levels, incident notification, support, opt-out,
Data return and accountability must correspond to technical processes. The design
Resilience includes an exit strategy: how to restore it in another environment, preserve evidence, and close the process.
Supplier without losing control. Known dependency can be managed; invisible dependency.
It becomes a surprise.

## GOVERNANCE, TESTING AND EFFECTIVENESS INDICATORS

Governance begins with the assignment of decisions. Service owners define criticality;
Technology translates requirements; security establishes controls; legal interprets obligations; management
Accepts residual risk. ISO/IEC 27001:2022 organizes information security as a system of
Risk-oriented management, people, policies, and technology. When roles become blurred, objectives
They become lists without authority. A responsibility matrix should accompany the architecture and...
to be reviewed with her.

Tests need to vary in depth. Automated integrity checks can be performed daily;
File restoration, frequent; application recovery, periodic; disaster recovery exercise, more.
comprehensive and well-planned. Each layer answers different questions. To confuse a simple test with
Full validation creates confidence without equivalent evidence.
Table 7 distinguishes the test layers by the question each one answers and, above all, by...
This question leaves the question open-ended, explaining why automatic verification does not replace practice.
full.

This is an open access article published under the Creative Commons Attribution license, which allows its use.
Distribution and reproduction in any medium, without restrictions, provided the original work is properly cited.

Machine Translated by Google
RGMOS - Multidisciplinary Scientific Journal
Knowledge. ISSN: 2675-9128. São Paulo-SP.

Year VII, v.2 2026 | Submission: October 8, 2026 | Accepted: October 10, 2026 | Publication: October 13, 2026

Table 7 - Test layers, reference frequency and generated evidence

| Test layer | Scope verified | Frequency of reference | Evidence generated | Question that no answer |
|---|---|---|---|---|
| Verification of integrity | Hash, reading and catalog | Daily | Legible copy and full | If the application restart |
| Restoration of files | Items and directories | Weekly | Recovery functional granular | If the service full returns |
| Recovery of application | Service with its dependencies | Quarterly | Consistency and sequence of ascent | If the team acts under pressure |
| Exercise of disaster | Site, identity, network and people | Annual | Observed time and real bottlenecks | Changes events that occurred after exercise |

Source: own elaboration based on CIS (2021), CISA (2023) and ISO 22301:2019.

CIS Controls v8 includes data recovery among its essential controls and emphasizes process.
Documented, automated backups, protection, and testing. The strength of this approach lies in...
Operationalization. Instead of treating continuity as an intention, it requires observable safeguards.
Responsible use, however, adapts frequency and scope to risk, without ultimately transforming the checklist.
Indicators should enable action. Job success rate is useful for operations, but insufficient for...
Governance. Coverage by criticality, approved restorations, real-time versus RTO, point.
Recovered versus RPO, exceptions won, and concentration by fault domain offer a reading
More comprehensive. Trends matter more than an isolated portrait.

Table 8 summarizes the indicators discussed and associates each one with its corresponding measure and reading.
which allows governance to separate operational metrics from effectiveness metrics.

This is an open access article published under the Creative Commons Attribution license, which allows its use.
Distribution and reproduction in any medium, without restrictions, provided the original work is properly cited.

Machine Translated by Google


**Year VII, v.2 2026 | Submission: October 8, 2026 | Accepted: October 10, 2026 | Publication: October 13, 2026**

Table 8 - Data protection effectiveness indicators

| **Indicator** | **How to measure** | **Governance reading** |
|---|---|---|
| Coverage put criticality | Services protected on classified services, by class | It reveals hidden gaps by overall average |
| Age of the last copy valid | Time elapsed since the copy most recently verified | Brings the actual RPO closer to the target. declared |
| Restorations approved | Tests with acceptance criteria answered regarding tests performed | It measures recovery, not completion of task |
| Observed time versus RTO | Service return time in controlled exercise | Shows whether the objective is executable. |
| Point recovered versus RPO | Difference between the state obtained and the admitted loss | It exposes promises without a mechanism. corresponding |
| Overdue exceptions | Accepted deviations whose deadline is The correction has expired. | Indicates accumulated residual risk. |
| Concentration put fault domain | Copies that depend on the same identity, site or provider | It signals the potential spread of a unique event |

Source: own elaboration based on CIS (2021), ISO/IEC 27001:2022 and Swanson et al. (2010).

Figure 4 shows the projected growth in public cloud spending. The increase in scale
Economic factors reinforce the need for controls that accompany dispersion and dependence. One should not...
To conclude that higher spending generates higher risk in a linear fashion; the graph only contextualizes the speed.
of the market and the financial magnitude of architectural decisions.

This is an open access article published under the Creative Commons Attribution license, which allows its use.
Distribution and reproduction in any medium, without restrictions, provided the original work is properly cited.

Machine Translated by Google
RCMOS - Multidisciplinary Scientific Journal
Knowledge. ISSN: 2675-9128. São Paulo-SP.

Year VII, v.2 2026 | Submission: October 8, 2026 | Accepted: October 10, 2026 | Publication: October 13, 2026

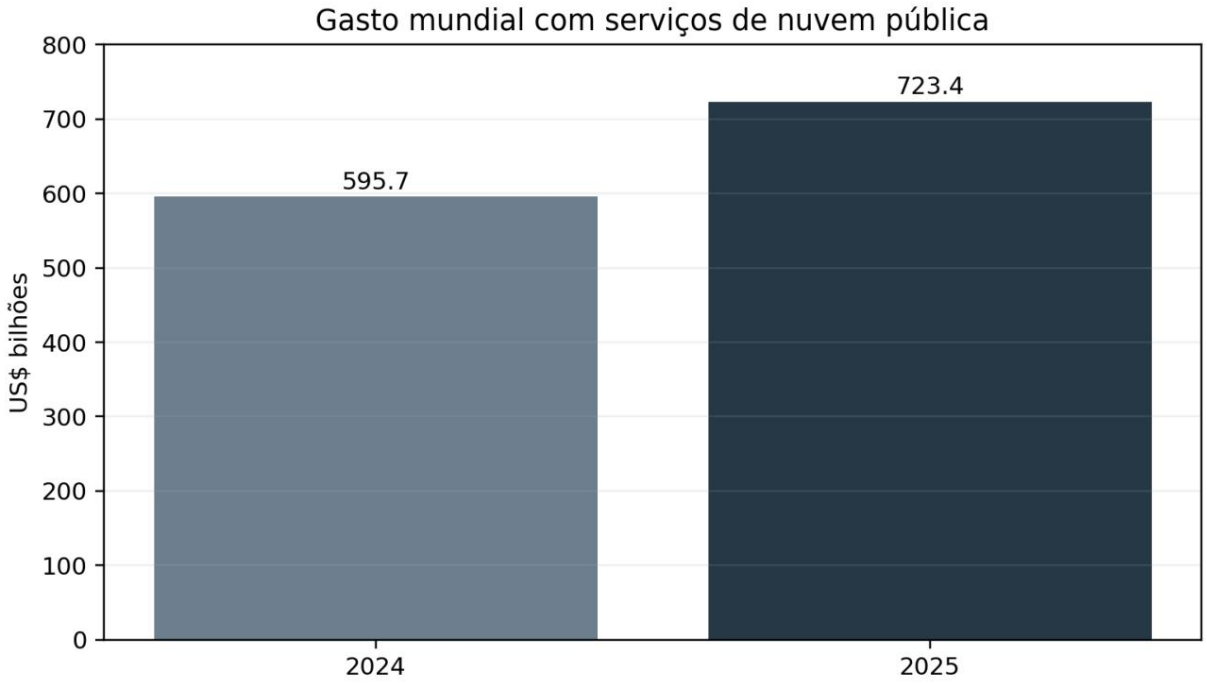



Figure 4 - Global end-user spending on public cloud services, 2024-2025. Source:
own elaboration with data from Gartner (2024).

Learning completes the cycle. Every test failure, relevant change, and incident should feed into the process.
Backlog with priority, responsible party, and deadline. Governance matures when deviations cease to exist.
These events can be episodes that lead to changes in patterns, contracts, and skills. Resilience is not a state of being.
definitive; it is a discipline of review in the face of systems that continue to change.

**FINAL CONSIDERATIONS**

The analysis demonstrates that data resilience cannot be purchased as an isolated attribute. It
emerges from the articulation between architecture, independent copies, protected identities, objectives
defined by the business, contracts, and people capable of executing them. The presence of redundancy or
Backup is a partial condition; the relevant property is the proven recovery of the service.
Technological evolution has expanded scale and flexibility, but has created management barriers. Environments
Hybrids combine different abstractions and responsibilities, so configuration errors and
Contractual loopholes can neutralize robust investments. Inventory and dependency maps.
They make this complexity visible and therefore manageable.
Ransomware highlights why availability and security have converged. An attacker seeks to achieve
Production and recovery mechanisms make a perimeter-focused defense insufficient.

This is an open access article published under the Creative Commons Attribution license, which allows its use.
Distribution and reproduction in any medium, without restrictions, provided the original work is properly cited.

Machine Translated by Google


**Year VII, v.2 2026 | Submission: October 8, 2026 | Accepted: October 10, 2026 | Publication: October 13, 2026**

Privilege separation, copy isolation, detection, and a clean restore area comprise a
a chain of events that needs to be rehearsed before the incident.

RPO and RTO offer a common language between technology and management when they are derived from analysis of
Impact. If defined without dependencies, budget, and testing, they become promises. Measure what is observed.
Working against the objective converts intention into evidence and allows for consciously negotiating cost, risk, and
priority.

The financial growth of the cloud does not eliminate organizational responsibilities. Providers
They offer important capabilities, but classification, retention, portability, and continuity are also important.
Costs remain shared or the client's responsibility, depending on the service. Contracts
They need to reflect the actual architecture and also provide for exit, investigation, and recovery.

Useful indicators prevent the comfort of averages. Segmented coverage by criticality, copy age.
Validity, restoration time, and exceptions reveal where the risk is concentrated. Panels should guide
Decisions and corrections; accumulating metrics without consequence only digitizes inertia.

The main managerial implication is to treat testing as knowledge production. Each exercise
It verifies assumptions, exposes bottlenecks, and trains coordination. Failures found in a controlled environment.
Results are valuable when they lead to correction. A culture that punishes unsuccessful testing tends to...
Concealing weaknesses until real disaster strikes.

For the purposes of this research, empirical comparisons between sectors, sizes, and cloud models remain possible.
Future studies may link governance maturity to observed recovery times and
Losses avoided, while preserving confidentiality. It is also worth examining how automation and
Artificial intelligence is altering detection, prioritization, and new failure modes.

In short, the correct question is not whether the organization has backups, but which services it can access.
Rebuild, but from what point, in what timeframe, under what conditions, and with what evidence.
When these responses are verified and reviewed, protection ceases to be merely a technological inventory and
It begins to function as an institutional capacity.

**REFERENCES**

ARMBRUST, Michael et al. A view of cloud computing. Communications of the ACM, New York, vol. 53, no. 4, p. 50-58, 2010. DOI: 10.1145/1721654.1721672.

CENTER FOR INTERNET SECURITY. CIS Critical Security Control 11: Data Recovery. East Greenbush: CIS, 2021. https://www.cisecurity.org/controls/data-recovery.

CHANDRAMOULI, Ramaswamy; PINHAS, Doron. Security Guidelines for Storage Infrastructure. NIST Special Publication 800-209. Gaithersburg: NIST, 2020. DOI: 10.6028/NIST.SP.800-209.

CISA. #StopRansomwareGuide. Washington, DC: Cybersecurity and Infrastructure Security Agency, 2023. https://www.cisa.gov/stopransomware/ransomware-guide.

ENISA. ENISA Threat Landscape 2024. Athens: European Union Agency for Cybersecurity, 2024. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024.

This is an open access article published under the Creative Commons Attribution license, which allows its use.
Distribution and reproduction in any medium, without restrictions, provided the original work is properly cited.

Machine Translated by Google


**Year VII, v.2 2026 | Submission: October 8, 2026 | Accepted: October 10, 2026 | Publication: October 13, 2026**

GARTNER. Gartner Forecasts Worldwide Public Cloud End-User Spending to Total $723 Billion in 2025. Stamford, 19 Nov. 2024. https://www.gartner.com/en/newsroom/press-releases/2024-11-19-gartner-forecasts-worldwide-public-cloud-end-user-spending-to-total-723-billion-dollars-in-2025.

GARTNER. Gartner Identifies the Top Trends Shaping the Future of Cloud. Stamford, May 13, 2025. https://www.gartner.com/en/newsroom/press-releases/2025-05-13-gartner-identifies-top-trends-shaping-the-future-of-cloud.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. ISO 22301:2019: Security and resilience - Business continuity management systems - Requirements. Geneva: ISO, 2019.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. ISO/IEC 27001:2022: Information security, cybersecurity and privacy protection - Information security management systems - Requirements. Geneva: ISO, 2022.

MELL, Peter; GRANCE, Timothy. The NIST Definition of Cloud Computing. NIST Special Publication 800-145. Gaithersburg: NIST, 2011. DOI: 10.6028/NIST.SP.800-145.

PATTERSON, David A.; GIBSON, Garth; KATZ, Randy H. A case for redundant arrays of inexpensive disks (RAID). In: ACM SIGMOD INTERNATIONAL CONFERENCE ON MANAGEMENT OF DATA, 1988, Chicago. Proceedings [...]. New York: ACM, 1988. p. 109-116. DOI: 10.1145/50202.50214.

SWANSON, Marianne et al. Contingency Planning Guide for Federal Information Systems. NIST Special Publication 800-34 Rev. 1. Gaithersburg: NIST, 2010. DOI: 10.6028/NIST.SP.800-34r1.

This is an open access article published under the Creative Commons Attribution license, which allows its use.
Distribution and reproduction in any medium, without restrictions, provided the original work is properly cited.