Ano VII, v.2 2026 | submissão: 08/10/2026 | aceito: 10/10/2026 | publicação: 13/10/2026

Resiliência de dados em infraestruturas híbridas: arquitetura, proteção, recuperação e governança

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

Resiliencia de los datos en infraestructuras híbridas: arquitectura, protección, recuperación y gobernanza

Eduardo Eneas Pereira Nunes

Bacharel em Ciência da Computação pela Universidade Estadual Paulista "Júlio de Mesquita Filho" (Unesp), campus de São José do Rio Preto; Especializado Latu Sensu em Redes de Telecomunicações pela Universidade Federal de Minas Gerais; MBA em Gestão de Projetos pela Universidade de São Paulo (USP), campus de Piracicaba; Profissional de Tecnologia da Informação.

RESUMO

A continuidade de serviços digitais depende menos da existência abstrata de uma cópia de segurança do que da capacidade comprovada de restaurar dados, aplicações e dependências dentro de limites aceitos pelo negócio. Este artigo examina a resiliência de dados em infraestruturas híbridas, nas quais recursos locais, virtualizados e em nuvem formam cadeias técnicas e contratuais difíceis de observar como um todo. O problema de pesquisa consiste em determinar quais dimensões permitem avaliar uma arquitetura de proteção para além da aquisição de produtos.

Adotou-se revisão bibliográfica e documental de natureza qualitativa, apoiada em normas, publicações institucionais e literatura científica. A análise organiza seis dimensões: arquitetura de armazenamento, cópias e isolamento, ameaça cibernética, objetivos de recuperação, governança híbrida e validação operacional. Conclui-se que resiliência é propriedade sistêmica e mensurável, produzida pela coerência entre criticidade, desenho, controles, testes e aprendizagem. Capacidade contratada sem restauração exercitada permanece apenas uma expectativa.

Palavras-chave: resiliência de dados; armazenamento; backup; recuperação de desastres; nuvem híbrida; governança.

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.

INTRODUÇÃO

A informação digital ocupa uma posição paradoxal nas organizações contemporâneas. Ela sustenta transações, logística, relações com clientes, pesquisa e decisões administrativas, mas sua utilidade

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

Ano VII, v.2 2026 | submissão: 08/10/2026 | aceito: 10/10/2026 | publicação: 13/10/2026

depende de uma infraestrutura que costuma desaparecer do campo de visão enquanto funciona. Uma interrupção torna visíveis, de uma só vez, dependências entre armazenamento, identidade, rede, aplicações e pessoas. O custo não decorre apenas da perda de arquivos; inclui paralisação, reconstrução, investigação, obrigações legais e erosão de confiança.

A expansão da nuvem amplia capacidade e flexibilidade, sem abolir o problema da continuidade. O Gartner estimou que o gasto mundial de usuários finais com serviços de nuvem pública passaria de US$ 595,7 bilhões em 2024 para US$ 723,4 bilhões em 2025, crescimento de 21,5% (GARTNER, 2024). O mesmo movimento distribui dados por regiões, contas, provedores e modelos de responsabilidade. Complexidade arquitetural, e não escassez de tecnologia, torna-se uma fonte central de exposição.

O NIST (*National Institute of Standards and Technology*, ou Instituto Nacional de Padrões e Tecnologia) – agência do governo dos Estados Unidos vinculada ao Departamento de Comércio – descreve a evolução do armazenamento desde serviços de bloco, arquivo e objeto até abstrações definidas por software e acesso em nuvem. Para Chandramouli e Pinhas (2020), esse percurso aumenta a complexidade de gestão e a probabilidade de erros de configuração. A observação afasta uma leitura puramente capacitista: mais cópias ou mais terabytes não significam, por si, maior segurança. Controles de acesso, isolamento, criptografia, integridade e restauração precisam compor um desenho coerente.

Diante desse cenário, o artigo pergunta como avaliar a resiliência de dados em ambientes híbridos sem reduzi-la à compra de backup. O objetivo é construir uma síntese analítica que relacione arquitetura, ameaça, recuperação, governança e evidência operacional. Não se pretende comparar fornecedores nem relatar experiências profissionais individuais. A contribuição está em converter recomendações dispersas em critérios que possam orientar projeto, auditoria e pesquisa aplicada.

METODOLOGIA

A pesquisa é qualitativa, exploratória e baseada em revisão bibliográfica e documental. Foram selecionadas publicações científicas clássicas sobre computação em nuvem, redundância e sistemas distribuídos, além de normas e guias técnicos produzidos por NIST, ISO, CISA, ENISA, CIS, IBM e Gartner. A combinação permite aproximar fundamentos duradouros de dados recentes sobre mercado e ameaças.

A busca conceitual priorizou os descritores *data resilience, storage security, backup, disaster recovery, business continuity, hybrid cloud, ransomware e recovery objectives*. A inclusão exigiu autoria identificável, vínculo institucional ou publicação acadêmica reconhecida, data e endereço

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

Ano VII, v.2 2026 | submissão: 08/10/2026 | aceito: 10/10/2026 | publicação: 13/10/2026

persistente ou DOI (*Digital Object Identifier*, ou Identificador de Objeto Digital) – código alfanumérico único e persistente usado para identificar documentos e arquivos digitais. Conteúdos comerciais foram usados apenas quando apresentavam pesquisa declarada ou números de mercado atribuíveis, nunca como prova suficiente de eficácia de um produto.

O corpus foi lido por categorias. A primeira reúne estrutura e redundância; a segunda trata proteção, isolamento e imutabilidade; a terceira cobre risco cibernético; a quarta examina continuidade, RPO e RTO; a quinta aborda nuvem híbrida e responsabilidade compartilhada; a sexta discute testes, indicadores e aprendizagem. Afirmações foram confrontadas entre tipos de fonte para reduzir dependência de uma única instituição.

A Tabela 1 sintetiza essa organização e explicita a correspondência entre cada dimensão, a pergunta que orienta sua leitura e as fontes predominantes, tornando o percurso analítico verificável.

Tabela 1 - Dimensões analíticas, perguntas orientadoras e fontes do corpus

Dimensão analítica	**Pergunta que orienta a leitura**	**Principais fontes mobilizadas**
Arquitetura de armazenamento	Como a disponibilidade é construída em camadas?	Patterson, Gibson e Katz (1988); Chandramouli e Pinhas (2020)
Cópias, isolamento e integridade	A cópia é recuperável e independente da produção?	Chandramouli e Pinhas (2020); CIS (2021)
Ameaça cibernética	O adversário alcança produção e recuperação?	ENISA (2024); CISA (2023)
Objetivos de recuperação	RPO e RTO derivam da análise de impacto no negócio?	Swanson et al. (2010); ISO 22301:2019
Governança híbrida	Quem responde por classificação, retenção e saída?	Mell e Grance (2011); Armbrust et al. (2010); Gartner (2024, 2025)
Validação operacional	Existe evidência de restauração testada e datada?	CIS (2021); ISO/IEC 27001:2022

Fonte: elaboração própria (2025).

Os valores financeiros são apresentados em dólares correntes e mantêm o recorte temporal da fonte. Previsões são identificadas como previsões, não como resultados realizados. O gráfico reproduz valores publicados pelo Gartner em novembro de 2024. Como limitações, destacam-se a rápida evolução tecnológica, diferenças regulatórias entre países e a ausência de dados primários de organizações específicas.

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

Ano VII, v.2 2026 | submissão: 08/10/2026 | aceito: 10/10/2026 | publicação: 13/10/2026

As tabelas e as figuras deste artigo foram elaboradas pelo autor. Quando reproduzem dados de fonte primária, a origem é indicada na própria legenda; quando organizam o conteúdo discutido na revisão, são sínteses analíticas, e os valores de referência têm caráter ilustrativo, sem pretensão de medição empírica.

A interpretação adota uma lógica sociotécnica. Controles são avaliados em relação a pessoas, processos, contratos e objetivos do negócio, evitando supor que a presença de uma ferramenta demonstre funcionamento. A validade analítica decorre da rastreabilidade das fontes e da consistência entre categorias, não de generalização estatística. Estudos empíricos futuros poderão testar o modelo em setores e portes distintos.

ARQUITETURA DE ARMAZENAMENTO E A CONSTRUÇÃO DA DISPONIBILIDADE

A disponibilidade moderna resulta de camadas, não de um componente infalível. O trabalho clássico de Patterson, Gibson e Katz (1988) mostrou como arranjos de discos poderiam combinar desempenho e tolerância a falhas por meio de redundância. A ideia permanece relevante, mas precisa ser situada: RAID (*Redundant Array of Independent Disks*, ou Conjunto Redundante de Discos Independentes) protege contra determinadas falhas de mídia; não substitui cópias independentes, histórico de versões ou recuperação após comprometimento lógico.

A passagem do armazenamento diretamente conectado para redes, sistemas distribuídos, hiperconvergência e serviços em nuvem aumentou opções de escala. Também multiplicou planos de controle, credenciais e interfaces. Chandramouli e Pinhas (2020) recomendam que a segurança considere autenticação, autorização, configuração, proteção de mídia, isolamento, criptografia e resposta. O objeto protegido já não é apenas o volume; inclui metadados e mecanismos que tornam o volume utilizável.

Redundância e recuperabilidade pertencem a categorias diferentes. Réplicas síncronas podem manter o serviço diante da falha de um nó, mas também propagam exclusões, corrupção ou ações maliciosas. Cópias versionadas preservam estados anteriores, embora possam permanecer inacessíveis se compartilham credenciais ou domínio administrativo com a produção. Uma arquitetura madura combina mecanismos com modos de falha distintos.

A Tabela 2 organiza essa distinção, relacionando cada mecanismo às falhas que efetivamente cobre, aos limites que preserva e ao papel que desempenha na recuperação do serviço.

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

Ano VII, v.2 2026 | submissão: 08/10/2026 | aceito: 10/10/2026 | publicação: 13/10/2026

Tabela 2 - Mecanismos de proteção: falhas cobertas, limites e papel na recuperação

Mecanismo	**Protege contra**	**Não protege contra**	**Papel na recuperação**
RAID e proteção de mídia	Falha de disco, setor defeituoso	Exclusão lógica, corrupção, acesso com credencial válida	Mantém o serviço disponível; não cria histórico
Réplica síncrona	Falha de nó, controlador ou sítio	Propagação imediata de exclusão e corrupção	Sustenta a operação; não oferece ponto de retorno
Snapshot no mesmo sistema	Erro recente de usuário ou aplicação	Perda do sistema que hospeda o snapshot	Retorno rápido para janelas curtas
Backup versionado em outro domínio	Exclusão, corrupção e perda de sítio	Credencial privilegiada compartilhada com a produção	Base do ponto de recuperação histórico
Cópia imutável (WORM)	Alteração e exclusão durante a retenção	Dado já cifrado antes de ser copiado	Assegura a persistência da versão preservada
Cópia offline ou isolada (air gap)	Ataque que alcança o plano de controle	Janela de perda maior e restauração mais lenta	Último recurso confiável da cadeia

Fonte: elaboração própria a partir de Patterson, Gibson e Katz (1988) e Chandramouli e Pinhas (2020).

A Figura 1 converte a mesma leitura em uma matriz de cobertura. A diagonal incompleta evidencia o argumento central: nenhum mecanismo isolado responde a todos os modos de falha, e a resiliência decorre da combinação de controles com falhas independentes entre si.

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

Ano VII, v.2 2026 | submissão: 08/10/2026 | aceito: 10/10/2026 | publicação: 13/10/2026

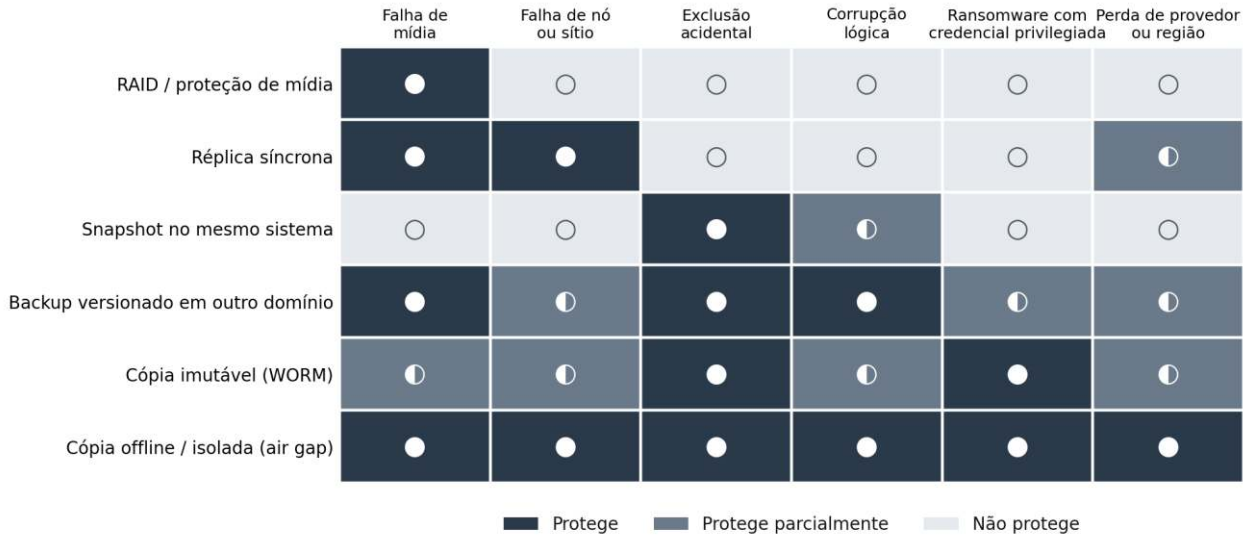

Figura 1 - Matriz de cobertura entre mecanismos de proteção e modos de falha. Fonte: elaboração própria (2025).

Outro ponto é a granularidade. Aplicações transacionais exigem consistência entre bancos, filas, arquivos e catálogos; copiar cada componente em instantes desconexos pode produzir um conjunto impossível de reiniciar. Por isso, proteção deve partir de mapas de dependência e estados consistentes. O desenho físico só adquire sentido quando relacionado à sequência lógica de restauração do serviço.

Classificação de dados evita tratar tudo da mesma maneira. Criticidade, frequência de mudança, retenção legal, sensibilidade e custo de recomposição orientam políticas diferentes. Uma base operacional pode exigir baixa perda admissível, enquanto um repositório histórico tolera janela maior. A diferenciação contém custos e impede que prioridades reais se dissolvam em uma política uniforme.

A arquitetura deve, enfim, registrar premissas. Volume, taxa de crescimento, janela de proteção, largura de banda, dependências e responsabilidades precisam ser mensuráveis. Sem esse inventário, a capacidade é dimensionada pelo passado e falha silenciosamente diante do crescimento. Projeto resiliente é aquele cuja adequação pode ser recalculada quando o ambiente muda.

CÓPIAS, ISOLAMENTO E INTEGRIDADE

Backup é um processo de preservação orientado à recuperação, não um depósito de arquivos. Sua qualidade depende da cobertura, da consistência, da retenção e da possibilidade de localizar versões úteis. Taxas elevadas de conclusão de tarefas podem esconder aplicações excluídas, credenciais expiradas ou cópias logicamente inconsistentes. O indicador central deve se aproximar do resultado restaurável.

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

Ano VII, v.2 2026 | submissão: 08/10/2026 | aceito: 10/10/2026 | publicação: 13/10/2026

A separação entre domínios de falha constitui princípio decisivo. Se produção e cópias dependem das mesmas identidades privilegiadas, uma credencial comprometida pode alcançar ambos. Isolamento físico, lógico ou temporal reduz essa propagação. O NIST (2020) inclui proteção, isolamento e garantia de restauração entre as recomendações específicas para infraestrutura de armazenamento.

A Tabela 3 compara estratégias de composição de cópias amplamente referenciadas na prática operacional, mostrando o que cada arranjo acrescenta e qual limite permanece depois de adotá-lo.

Tabela 3 - Estratégias de composição de cópias: o que reforçam e o que não resolvem

Estratégia	**Composição**	**O que reforça**	**Limite que permanece**
3-2-1	Três cópias, dois tipos de mídia, uma fora do sítio	Diversidade de mídia e dispersão geográfica	Não exige imutabilidade nem verificação de integridade
3-2-1-1-0	Acrescenta uma cópia imutável ou offline e nenhum erro na verificação	Resistência a ransomware e evidência de cópia legível	Custo e complexidade da gestão de retenção
4-3-2	Quatro cópias, três locais, duas fora do sítio	Redundância adicional para ambientes regulados	Exige orquestração e testes contínuos

Fonte: elaboração própria a partir de CISA (2023) e CIS (2021).

Imutabilidade acrescenta resistência à alteração durante uma janela definida, mas não corrige retenção inadequada nem garante que o conteúdo seja limpo. Uma cópia imutável de dados já cifrados pelo invasor preserva o dano. O controle precisa ser associado a detecção, versões anteriores e análise do ponto de recuperação. Tecnologia útil torna-se perigosa quando seu rótulo substitui a compreensão do mecanismo.

Criptografia protege confidencialidade em trânsito e repouso, porém introduz dependência de chaves. Chaves indisponíveis transformam uma cópia íntegra em dado inutilizável; chaves expostas anulam parte da proteção. Gestão de ciclo de vida, segregação de funções, rotação e recuperação segura devem integrar o mesmo plano. A segurança do backup inclui a segurança de seus meios de acesso.

A integridade requer verificação contínua. Hashes e validações detectam alterações, mas apenas testes de leitura e restauração revelam problemas de catálogo, encadeamento ou compatibilidade. A automação pode ampliar amostragem e frequência, desde que falhas produzam tratamento e não apenas alertas acumulados. Evidência operacional precisa ter responsável, prazo e critério de aceite.

Retenção também possui dimensão econômica e jurídica. Manter tudo indefinidamente aumenta custo, superfície de exposição e complexidade de busca; eliminar cedo demais compromete recuperação e obrigações. Políticas devem conciliar necessidade de negócio, legislação, litígios

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

Ano VII, v.2 2026 | submissão: 08/10/2026 | aceito: 10/10/2026 | publicação: 13/10/2026

previsíveis e minimização. O resultado é uma matriz de retenção justificável, revisada e vinculada à classificação dos dados.

RANSOMWARE E RESILIÊNCIA CIBERNÉTICA

O ransomware transformou recuperação em problema de segurança estratégica. O panorama da ENISA (*European Union Agency for Cybersecurity*, ou Agência da União Europeia para a Cibersegurança) para 2024 colocou ameaças à disponibilidade no topo e ransomware logo em seguida, a partir da análise de milhares de incidentes divulgados. O dado sugere que confidencialidade não basta: a organização precisa sustentar ou reconstruir serviços sob pressão e com informação incompleta.

A Figura 2 detalha essa distribuição. Ameaças à disponibilidade e ransomware respondem, somadas, por cerca de dois terços dos incidentes analisados, e as ameaças a dados ocupam a terceira posição. O perfil reforça a leitura do artigo: a maior parte do volume observado ataca justamente a capacidade de operar e de retornar.

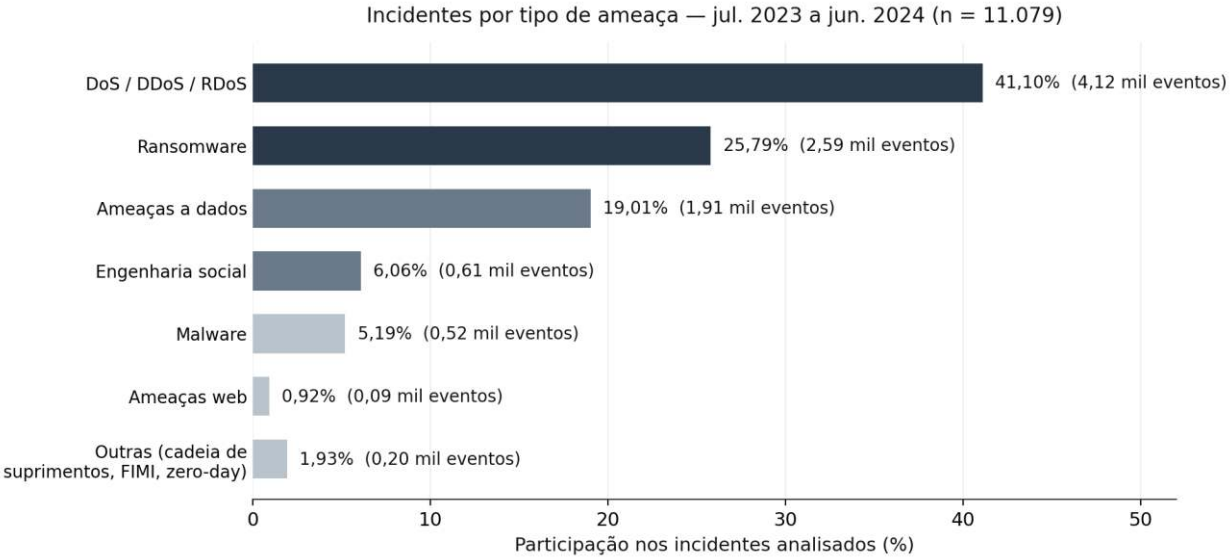

Figura 2 - Distribuição dos incidentes analisados por tipo de ameaça, julho de 2023 a junho de 2024. Fonte: elaboração própria com dados da ENISA (2024).

Ataques modernos procuram credenciais, consoles administrativos, hipervisores e repositórios de cópia. A defesa não pode supor um perímetro intacto. Privilégio mínimo, autenticação forte, segregação de contas, caminhos administrativos protegidos e registro de ações reduzem a chance de um único acesso dominar toda a cadeia. O desenho deve considerar o adversário já presente.

A Tabela 4 relaciona os alvos mais recorrentes na cadeia de recuperação, o efeito pretendido pelo atacante, o controle prioritário e a evidência que permite afirmar que o controle está em operação.

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

Ano VII, v.2 2026 | submissão: 08/10/2026 | aceito: 10/10/2026 | publicação: 13/10/2026

Tabela 4 - Alvos do ransomware na cadeia de recuperação e controles correspondentes

Alvo na cadeia	**Objetivo do atacante**	**Controle prioritário**	**Evidência esperada**
Identidade e contas privilegiadas	Obter acesso administrativo amplo	Privilégio mínimo, autenticação forte, contas separadas	Inventário de contas privilegiadas revisado
Console de backup	Reduzir retenção, apagar jobs e catálogos	Domínio administrativo distinto e aprovação dupla	Registro de alterações de política de retenção
Hipervisor e plano de controle	Cifrar muitos serviços de uma só vez	Rede de gestão segregada e registro de ações	Trilha de auditoria com revisão periódica
Repositório de cópias	Impedir o retorno a estados anteriores	Imutabilidade, cópia isolada e credenciais próprias	Restauração testada a partir da cópia isolada
Snapshots e réplicas	Eliminar pontos de retorno recentes	Retenção fora do alcance da conta de produção	Verificação automática de existência e idade
Chaves de criptografia	Tornar inutilizável a cópia íntegra	Custódia segregada, rotação e cópia de recuperação	Exercício documentado de recuperação de chaves

Fonte: elaboração própria a partir de CISA (2023), ENISA (2024) e Chandramouli e Pinhas (2020).

A CISA (*Cybersecurity and Infrastructure Security Agency*, ou Agência de Segurança Cibernética e de Infraestrutura) recomenda backups offline, criptografados e testados como parte da resposta ao ransomware. A palavra “testados” altera o foco: armazenar não equivale a recuperar. Exercícios precisam verificar dados, sequência de subida, identidades, redes, chaves e capacidade das equipes. Um arquivo restaurado com sucesso não demonstra que o serviço inteiro voltará no prazo necessário.

A detecção deve alcançar o plano de dados. Mudanças abruptas na taxa de modificação, compressão, exclusões ou comportamento de contas podem indicar ataque antes do bloqueio total. Entretanto, limiares rígidos produzem falsos positivos em rotinas legítimas. A linha de base deve conhecer ciclos de fechamento, cargas analíticas e manutenções para distinguir anomalia de sazonalidade.

Recuperar em ambiente comprometido pode reiniciar o incidente. É necessário definir área limpa, critérios de confiança e etapas de validação antes de reconectar sistemas. Imagens, configurações e

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

Ano VII, v.2 2026 | submissão: 08/10/2026 | aceito: 10/10/2026 | publicação: 13/10/2026

credenciais precisam ser examinadas; dependências externas, reautorizadas. A velocidade importa, mas uma restauração precipitada pode ampliar o tempo total de indisponibilidade.

Comunicação integra a resiliência. Decisões sobre parada, priorização, notificação e retomada envolvem direção, jurídico, segurança, operações e áreas de negócio. Papéis previamente definidos reduzem disputa durante a crise. Depois do evento, a análise deve transformar evidências em correções arquiteturais e processuais, fechando o ciclo entre incidente e aprendizagem.

RPO, RTO E CONTINUIDADE ORIENTADA AO NEGÓCIO

Dois parâmetros organizam a conversa sobre recuperação. O recovery point objective, RPO, exprime a perda máxima de dados admitida em tempo; o recovery time objective, RTO, indica o prazo desejado para restabelecimento. Ambos são objetivos, não características automáticas de uma ferramenta. Precisam derivar do impacto sobre processos e ser confrontados com capacidade técnica real.

Swanson et al. (2010) situam o planejamento de contingência no ciclo de vida dos sistemas e recomendam avaliar operações para determinar prioridades. A análise de impacto no negócio fornece essa ligação. Ela identifica serviços essenciais, dependências, efeitos da interrupção e tolerâncias. Sem tal base, RPO e RTO tendem a refletir conveniência técnica ou ambição sem orçamento.

Objetivos agressivos têm custos. Reduzir a perda admissível pode exigir replicação frequente, maior largura de banda e mecanismos consistentes de captura. Diminuir o tempo de retorno demanda capacidade reservada, automação e equipes treinadas. O equilíbrio não é escolher entre segurança e economia, mas explicitar quanto custa cada nível e qual perda ele pretende limitar.

A Tabela 5 ilustra como a classificação de criticidade traduz essa negociação em parâmetros distintos por classe de serviço, evitando política uniforme para necessidades desiguais.

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

Ano VII, v.2 2026 | submissão: 08/10/2026 | aceito: 10/10/2026 | publicação: 13/10/2026

Tabela 5 - Classes de criticidade, objetivos de referência e mecanismos associados

Classe	**Exemplo de serviço**	**RPO / RTO de referência**	**Mecanismo predominante**	**Custo relativo**
Crítica	Transação on-line, atendimento ao cliente	Minutos / até 1 hora	Replicação contínua com cópia imutável	Muito alto
Essencial	ERP, faturamento, integrações	Até 1 hora / até 4 horas	Réplica assíncrona e backup frequente	Alto
Importante	Colaboração, relatórios internos	Até 12 horas / até 24 horas	Backup diário versionado	Moderado
De suporte	Repositório histórico, arquivos frios	Até 24 horas / até 72 horas	Backup periódico com retenção longa	Baixo

Fonte: elaboração própria a partir de Swanson et al. (2010) e da ISO 22301:2019. Os intervalos são ilustrativos e devem ser derivados da análise de impacto no negócio de cada organização.

A Figura 3 representa a tendência que sustenta essa diferenciação. À medida que os objetivos se tornam mais rigorosos, o custo cresce de forma acentuada, o que explica por que exigências uniformes tendem a ser abandonadas na prática ou financiadas apenas no discurso.

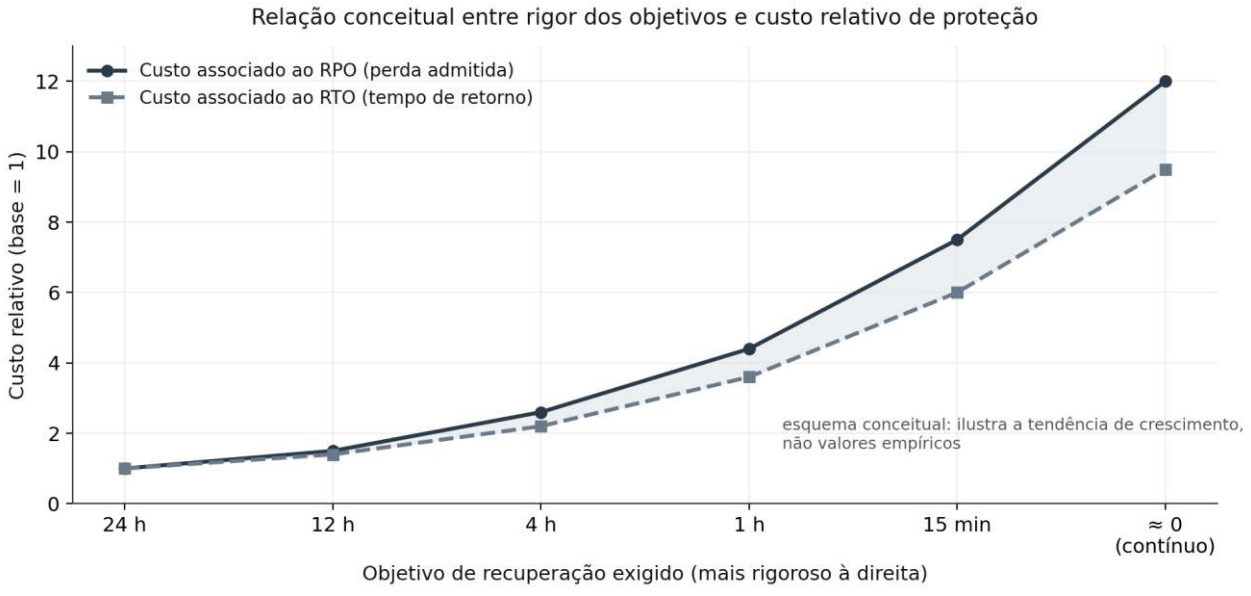

Figura 3 - Relação conceitual entre o rigor dos objetivos de recuperação e o custo relativo de proteção. Fonte: elaboração própria (2025); esquema conceitual, sem valores empíricos.

A recuperação ocorre em sequência. Identidade, rede, serviços de nomes, bancos e integrações podem preceder a aplicação visível ao usuário. Medir apenas o tempo de restauração do volume subestima a

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

Ano VII, v.2 2026 | submissão: 08/10/2026 | aceito: 10/10/2026 | publicação: 13/10/2026

duração do serviço. Mapas de dependência e runbooks ordenados transformam RTO em plano executável e permitem localizar gargalos antes de uma crise.

A ISO 22301:2019 trata continuidade como sistema de gestão, com política, análise, estratégia, planos, exercícios e melhoria. Essa estrutura evita que recuperação seja evento anual isolado. Mudanças de arquitetura, equipe ou fornecedor devem acionar revisão dos planos. O objetivo permanece estável somente enquanto suas premissas continuam verdadeiras.

Métricas precisam distinguir intenção de evidência. Cobertura de aplicações, idade da última cópia válida, percentual de restaurações aprovadas, tempo observado e divergência em relação ao objetivo compõem uma visão mais honesta. Resultados devem ser segmentados por criticidade; uma média geral pode esconder justamente o serviço que não pode falhar.

NUVEM HÍBRIDA, PORTABILIDADE E RESPONSABILIDADE

A definição de nuvem do NIST destaca acesso sob demanda a um conjunto compartilhado de recursos configuráveis (MELL; GRANCE, 2011). O modelo desloca parte da operação para o provedor, mas não transfere automaticamente classificação, retenção, identidade e continuidade. Responsabilidades variam por serviço e contrato. Presumi-las é um risco recorrente.

A Tabela 6 explicita essa variação por modelo de serviço e mostra que classificação, teste de restauração e portabilidade permanecem com o cliente em todos os arranjos, ainda que a operação subjacente mude de mãos.

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

Ano VII, v.2 2026 | submissão: 08/10/2026 | aceito: 10/10/2026 | publicação: 13/10/2026

Tabela 6 - Distribuição de responsabilidades por modelo de serviço

Item da proteção	**Instalação local**	**IaaS**	**PaaS**	**SaaS**
Infraestrutura física	Cliente	Provedor	Provedor	Provedor
Configuração do serviço	Cliente	Cliente	Compartilhada	Provedor
Classificação dos dados	Cliente	Cliente	Cliente	Cliente
Identidade e acesso	Cliente	Cliente	Compartilhada	Compartilhada
Cópia e retenção	Cliente	Cliente	Compartilhada	Depende do contrato
Gestão de chaves	Cliente	Cliente ou compartilhada	Compartilhada	Provedor ou opcional
Teste de restauração	Cliente	Cliente	Cliente	Cliente
Portabilidade e saída	Cliente	Compartilhada	Compartilhada	Depende do contrato

Fonte: elaboração própria a partir de Mell e Grance (2011) e Armbrust et al. (2010). A atribuição efetiva depende do contrato e do serviço contratado.

Armbrust et al. (2010) identificaram elasticidade e economia de escala como forças da computação em nuvem, ao lado de obstáculos como disponibilidade, aprisionamento e confidencialidade. Em ambientes híbridos, essas tensões se acumulam. Dados podem circular entre instalações próprias, software como serviço e múltiplas regiões, cada qual com mecanismos diferentes de proteção e exportação.

Portabilidade deve ser testada, não inferida de cláusulas genéricas. Formatos, APIs, metadados, chaves e taxas de saída influenciam a possibilidade de recuperar ou migrar. Uma cópia armazenada no mesmo serviço pode responder a exclusões acidentais, mas oferecer pouca independência diante de indisponibilidade ampla ou encerramento contratual. O cenário determina o grau de separação necessário.

A soberania adiciona jurisdição e localização ao desenho. Regras de privacidade, acesso governamental e transferência internacional podem limitar regiões e operadores. O Gartner (2025) apontou soberania digital entre as tendências que moldariam a nuvem e previu crescimento expressivo de estratégias específicas em multinacionais até 2029. Previsões não são fatos consumados, mas sinalizam pressão de governança.

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

Ano VII, v.2 2026 | submissão: 08/10/2026 | aceito: 10/10/2026 | publicação: 13/10/2026

Custos variáveis exigem observabilidade financeira. Armazenamento, requisições, recuperação e transferência podem mudar o custo total conforme retenção e exercícios. A otimização que reduz cópias ou testes para poupar despesa pode aumentar exposição operacional. FinOps aplicado à proteção deve relacionar gasto a criticidade, cobertura e evidência de recuperação.

Contratos completam a arquitetura. Níveis de serviço, notificação de incidente, suporte, exclusão, devolução de dados e responsabilidade precisam corresponder aos processos técnicos. O desenho resiliente inclui uma saída: como restaurar em outro ambiente, preservar evidências e encerrar o fornecedor sem perder controle. Dependência conhecida pode ser administrada; dependência invisível torna-se surpresa.

GOVERNANÇA, TESTES E INDICADORES DE EFETIVIDADE

Governança começa pela atribuição de decisões. Proprietários de serviço definem criticidade; tecnologia traduz requisitos; segurança estabelece controles; jurídico interpreta obrigações; direção aceita risco residual. A ISO/IEC 27001:2022 organiza a segurança da informação como sistema de gestão orientado a riscos, pessoas, políticas e tecnologia. Quando papéis se confundem, objetivos tornam-se listas sem autoridade. Uma matriz de responsabilidade deve acompanhar a arquitetura e ser revisada com ela.

Testes precisam variar em profundidade. Verificação automática de integridade pode ser diária; restauração de arquivos, frequente; recuperação de aplicação, periódica; exercício de desastre, mais amplo e planejado. Cada camada responde a perguntas diferentes. Confundir um teste simples com validação completa cria confiança sem evidência equivalente.

A Tabela 7 distingue as camadas de teste pela pergunta que cada uma responde e, sobretudo, pela pergunta que deixa em aberto, explicitando por que a verificação automática não substitui o exercício completo.

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

Ano VII, v.2 2026 | submissão: 08/10/2026 | aceito: 10/10/2026 | publicação: 13/10/2026

Tabela 7 - Camadas de teste, frequência de referência e evidência gerada

Camada de teste	**Escopo verificado**	**Frequência de referência**	**Evidência gerada**	**Pergunta que não responde**
Verificação de integridade	Hash, leitura e catálogo	Diária	Cópia legível e íntegra	Se a aplicação reinicia
Restauração de arquivos	Itens e diretórios	Semanal	Recuperação granular funcional	Se o serviço completo retorna
Recuperação de aplicação	Serviço com suas dependências	Trimestral	Consistência e sequência de subida	Se a equipe atua sob pressão
Exercício de desastre	Sítio, identidade, rede e pessoas	Anual	Tempo observado e gargalos reais	Mudanças ocorridas após o exercício

Fonte: elaboração própria a partir de CIS (2021), CISA (2023) e da ISO 22301:2019.

O CIS Controls v8 inclui recuperação de dados entre seus controles essenciais e enfatiza processo documentado, cópias automatizadas, proteção e testes. A força dessa abordagem está na operacionalização. Em vez de tratar continuidade como intenção, ela exige salvaguardas observáveis. O uso responsável, contudo, adapta frequência e escopo ao risco, sem transformar checklist enfim.

Indicadores devem permitir ação. Taxa de sucesso de jobs é útil para operação, mas insuficiente para governança. Cobertura por criticidade, restaurações aprovadas, tempo real versus RTO, ponto recuperado versus RPO, exceções vencidas e concentração por domínio de falha oferecem uma leitura mais completa. Tendências importam mais que um retrato isolado.

A Tabela 8 reúne os indicadores discutidos e associa cada um à medida correspondente e à leitura que permite à governança, de modo a separar métricas de operação de métricas de efetividade.

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

Ano VII, v.2 2026 | submissão: 08/10/2026 | aceito: 10/10/2026 | publicação: 13/10/2026

Tabela 8 - Indicadores de efetividade da proteção de dados

Indicador	**Como medir**	**Leitura de governança**
Cobertura por criticidade	Serviços protegidos sobre serviços classificados, por classe	Revela lacunas escondidas pela média geral
Idade da última cópia válida	Tempo decorrido desde a cópia verificada mais recente	Aproxima o RPO real do objetivo declarado
Restaurações aprovadas	Testes com critério de aceite atendido sobre testes executados	Mede recuperação, não conclusão de tarefa
Tempo observado versus RTO	Duração do retorno do serviço em exercício controlado	Mostra se o objetivo é executável
Ponto recuperado versus RPO	Diferença entre o estado obtido e a perda admitida	Expõe promessas sem mecanismo correspondente
Exceções vencidas	Desvios aceitos cujo prazo de correção expirou	Indica risco residual acumulado
Concentração por domínio de falha	Cópias que dependem da mesma identidade, sítio ou provedor	Sinaliza propagação potencial de um único evento

Fonte: elaboração própria a partir de CIS (2021), ISO/IEC 27001:2022 e Swanson et al. (2010).

Figura 4 apresenta o crescimento previsto do gasto com nuvem pública. O aumento de escala econômica reforça a necessidade de controles que acompanhem dispersão e dependência. Não se deve concluir que gasto maior gera risco maior de forma linear; o gráfico apenas contextualiza a velocidade do mercado e a magnitude financeira das decisões de arquitetura.

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

Ano VII, v.2 2026 | submissão: 08/10/2026 | aceito: 10/10/2026 | publicação: 13/10/2026

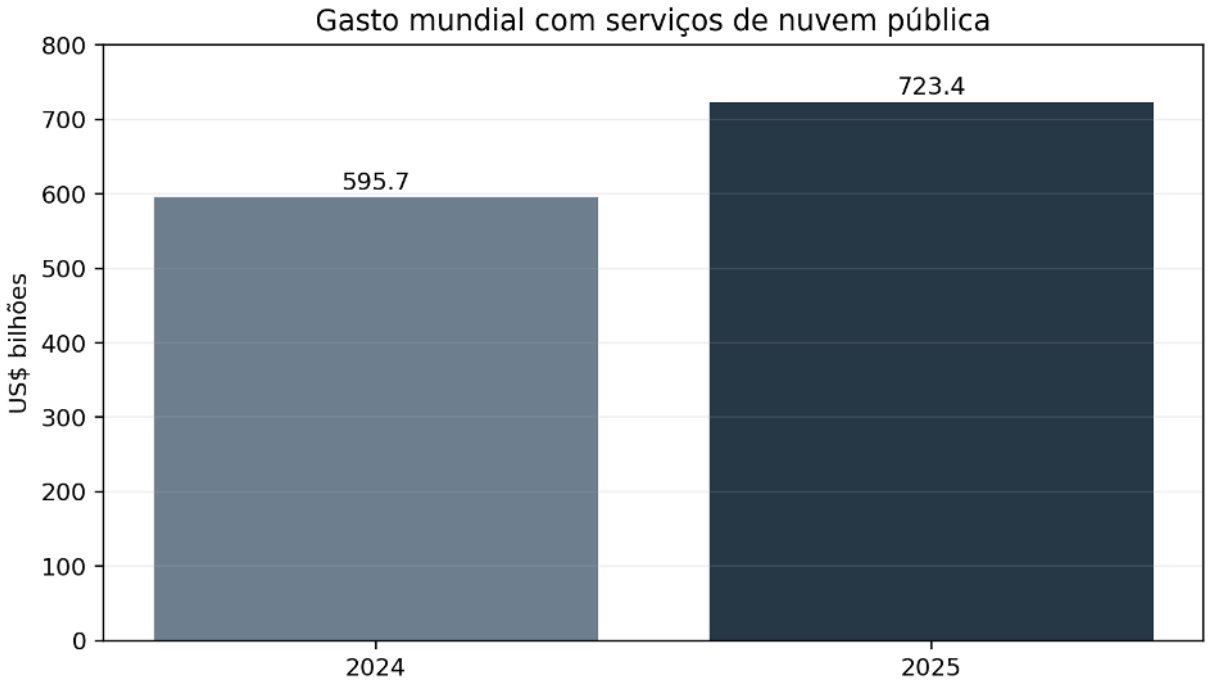

Figura 4 - Gasto mundial de usuários finais com serviços de nuvem pública, 2024-2025. Fonte: elaboração própria com dados do Gartner (2024).

Aprendizagem encerra o ciclo. Toda falha de teste, mudança relevante e incidente deve alimentar backlog com prioridade, responsável e prazo. A governança amadurece quando desvios deixam de ser episódios e passam a modificar padrões, contratos e capacitação. Resiliência não é estado definitivo; é disciplina de revisão diante de sistemas que continuam mudando.

CONSIDERAÇÕES FINAIS

A análise demonstra que resiliência de dados não pode ser comprada como atributo isolado. Ela emerge da articulação entre arquitetura, cópias independentes, identidades protegidas, objetivos definidos pelo negócio, contratos e pessoas capazes de executar. A presença de redundância ou backup é condição parcial; a propriedade relevante é a recuperação comprovada do serviço.

A evolução tecnológica ampliou escala e flexibilidade, mas criou superfícies de gestão. Ambientes híbridos combinam abstrações e responsabilidades diferentes, de modo que erros de configuração e lacunas contratuais podem neutralizar investimentos robustos. Inventário e mapas de dependência tornam essa complexidade visível e, portanto, administrável.

Ransomware evidencia porque disponibilidade e segurança convergiram. Um invasor procura atingir produção e mecanismos de recuperação, tornando insuficiente uma defesa concentrada no perímetro.

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

Ano VII, v.2 2026 | submissão: 08/10/2026 | aceito: 10/10/2026 | publicação: 13/10/2026

Separação de privilégios, isolamento das cópias, detecção e área limpa de restauração compõem uma cadeia que precisa ser ensaiada antes do incidente.

RPO e RTO oferecem linguagem comum entre tecnologia e gestão quando derivam de análise de impacto. Se definidos sem dependências, orçamento e teste, tornam-se promessas. Medir o observado contra o objetivo converte intenção em evidência e permite negociar conscientemente custo, risco e prioridade.

O crescimento financeiro da nuvem não elimina responsabilidades organizacionais. Provedores oferecem capacidades importantes, mas classificação, retenção, portabilidade e continuidade permanecem compartilhadas ou sob responsabilidade do cliente, conforme o serviço. Contratos precisam refletir a arquitetura real e prever também saída, investigação e recuperação.

Indicadores úteis evitam o conforto das médias. Cobertura segmentada por criticidade, idade da cópia válida, tempo de restauração e exceções revelam onde o risco se concentra. Painéis devem conduzir a decisões e correções; acumular métricas sem consequência apenas digitaliza a inércia.

A principal implicação gerencial é tratar testes como produção de conhecimento. Cada exercício verifica premissas, expõe gargalos e treina coordenação. Falhas encontradas em ambiente controlado são resultados valiosos quando geram correção. Uma cultura que pune o teste malsucedido tende a ocultar fragilidades até o desastre real.

Para a pesquisa, permanece aberta a comparação empírica entre setores, portes e modelos de nuvem. Estudos futuros podem relacionar maturidade de governança a tempos observados de recuperação e perdas evitadas, preservando confidencialidade. Também convém examinar como automação e inteligência artificial alteram detecção, priorização e novos modos de falha.

Em síntese, a pergunta correta não é se a organização possui backup, mas quais serviços consegue reconstruir, a partir de qual ponto, em quanto tempo, sob quais condições e com que evidência. Quando essas respostas são verificadas e revisadas, a proteção deixa de ser inventário tecnológico e passa a funcionar como capacidade institucional.

REFERÊNCIAS

ARMBRUST, Michael et al. A view of cloud computing. Communications of the ACM, New York, v. 53, n. 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. #StopRansomware Guide. 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.

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

Ano VII, v.2 2026 | submissão: 08/10/2026 | aceito: 10/10/2026 | publicação: 13/10/2026

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, 13 maio 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.

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.