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

Ano VII, v.2 2026 | submissão: 14/01/2026 | aceito: 17/01/2026 | publicação: 20/01/2026

Resiliência tecnológica em pequenas e médias empresas: continuidade operacional, backup e recuperação de ambientes de TI

Technology Resilience in Small and Medium-Sized Enterprises: Business Continuity, Backup and IT Environment Recovery

Resiliencia tecnológica en pequeñas y medianas empresas: continuidad del negocio, copias de seguridad y recuperación del entorno informático

Guilherme Gallo Zazeri

Profissional de Tecnologia da Informação, consultor e empreendedor em infraestrutura, conectividade e soluções tecnológicas, com mais de 25 anos de trajetória profissional.

Resumo

A dependência crescente de servidores, serviços em nuvem, redes e aplicações tornou a continuidade tecnológica uma condição de funcionamento para pequenas e médias empresas. Este artigo analisa a resiliência de TI a partir da identificação de ativos críticos, análise de impacto, estratégias de backup, testes de restauração, documentação e monitoramento. A pesquisa adota revisão narrativa estruturada de normas, guias técnicos, livros e relatórios institucionais verificáveis, com destaque para NIST CSF 2.0, NIST SP 800-34 Rev. 1, ISO 22301 e Verizon DBIR. A análise demonstra que possuir cópias de dados não equivale a possuir capacidade de recuperação: a continuidade depende de prioridades definidas, responsabilidades, cópias protegidas, testes periódicos e procedimentos executáveis. Para PMEs, o desafio central é construir controles proporcionais ao risco e à capacidade operacional, evitando tanto a ausência de planejamento quanto arquiteturas excessivamente complexas.

Palavras-chave: resiliência tecnológica; continuidade de negócios; backup; recuperação de desastres; pequenas e médias empresas; infraestrutura de TI.

Abstract

The growing dependence on servers, cloud services, networks, and applications has made technology continuity a basic operating condition for small and medium-sized enterprises. This article examines IT resilience through critical-asset identification, business impact analysis, backup strategies, restoration testing, documentation, and monitoring. The study adopts a structured narrative review of verifiable standards, technical guides, books, and institutional reports, with emphasis on NIST CSF 2.0, NIST SP 800-34 Rev. 1, ISO 22301, and the Verizon DBIR. The analysis shows that possessing data copies is not equivalent to possessing recovery capability: continuity depends on defined priorities, responsibilities, protected copies, periodic tests, and executable procedures. For SMEs, the central challenge is to build controls proportional to risk and operational capacity, avoiding both lack of planning and unnecessarily complex architectures.

Keywords: technology resilience; business continuity; backup; disaster recovery; small and medium-sized enterprises; IT infrastructure.

Introdução

A infraestrutura de tecnologia deixou de ser mero suporte administrativo para se tornar parte do funcionamento cotidiano de empresas de praticamente todos os setores. Sistemas de gestão, arquivos, e-mail, comunicação, acesso remoto e serviços em nuvem formam cadeias de dependência nas quais uma falha técnica pode interromper vendas, atendimento, faturamento ou produção. Whitman 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: 14/01/2026 | aceito: 17/01/2026 | publicação: 20/01/2026

Mattord (2021) observam que a segurança da informação precisa ser tratada em conexão com os objetivos organizacionais, e não como atividade isolada da área técnica.

Para pequenas e médias empresas, essa dependência convive frequentemente com equipes reduzidas e ambientes heterogêneos. O NIST publicou em 2024 um guia específico para pequenos negócios baseado no Cybersecurity Framework 2.0, reconhecendo que organizações com recursos modestos também precisam estruturar governança, identificação, proteção, detecção, resposta e recuperação (ELIOT, 2024). A questão, portanto, não é reproduzir a arquitetura de uma grande corporação, mas estabelecer prioridades compatíveis com o risco.

A continuidade operacional constitui uma dessas prioridades. Swanson et al. (2010), no NIST SP 800-34 Rev. 1, relacionam análise de impacto, controles preventivos, estratégias de recuperação, testes e manutenção a um programa consistente de contingência. A partir dessa base, este artigo examina seis dimensões da resiliência tecnológica em PMEs, com atenção especial à capacidade real de restaurar serviços depois de falhas, incidentes ou indisponibilidades.

2. Metodologia

O estudo utiliza revisão narrativa estruturada, adequada à integração de normas técnicas, literatura de segurança da informação, continuidade de negócios e evidências institucionais recentes. Foram priorizadas fontes com autoria, instituição responsável, edição e conteúdo identificáveis.

O núcleo normativo é formado pelo NIST Cybersecurity Framework 2.0, pelo NIST SP 1300 voltado a pequenos negócios, pelo NIST SP 800-34 Rev. 1 e pela ISO 22301:2019. Essas referências permitem distinguir gestão de risco, continuidade organizacional e recuperação de sistemas.

A literatura de Whitman e Mattord (2021) e Stallings (2018) foi empregada para contextualizar segurança, governança e controles. O Verizon Data Breach Investigations Report 2025 foi utilizado como fonte empírica contemporânea sobre incidentes e violações.

A seleção não foi orientada por marcas comerciais de hardware, hipervisores ou serviços em nuvem. O objetivo foi preservar aplicabilidade a ambientes tecnológicos distintos e evitar que recomendações de arquitetura fossem confundidas com preferência por fornecedor.

Os materiais foram organizados em seis eixos: criticidade, análise de impacto, backup, recuperação, documentação e monitoramento. Em cada eixo, buscou-se diferenciar existência de recurso técnico e capacidade operacional comprovada.

O artigo não propõe certificação, auditoria ou modelo universal de continuidade. As recomendações devem ser adaptadas ao porte, setor, requisitos regulatórios, orçamento, tolerância à indisponibilidade e criticidade dos dados de cada organização.

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: 14/01/2026 | aceito: 17/01/2026 | publicação: 20/01/2026

3.1 Dependência tecnológica e criticidade dos ativos

Uma estratégia de resiliência começa pela identificação do que realmente sustenta a operação. O NIST CSF 2.0 (PASCOE; QUINN; SCARFONE, 2024) inclui a função Identify justamente porque organizações precisam conhecer ativos, dependências e riscos antes de selecionar controles.

Inventários técnicos ganham valor quando associados a processos de negócio. Um servidor pode parecer apenas um equipamento, mas hospedar autenticação, arquivos ou aplicação indispensável ao faturamento. A criticidade deve ser definida pelo impacto da indisponibilidade, não pelo preço do ativo.

Swanson et al. (2010) relacionam o Business Impact Analysis à determinação de prioridades de recuperação. A análise ajuda a identificar quais sistemas sustentam funções essenciais e qual perda de disponibilidade pode ser tolerada.

Em PMEs, dependências ocultas são frequentes: credenciais mantidas por uma única pessoa, equipamentos sem documentação ou aplicações legadas cuja integração não é conhecida. A documentação técnica reduz esse risco ao transformar conhecimento tácito em informação organizacional.

A classificação também evita desperdício. Nem todos os serviços exigem o mesmo nível de redundância ou o mesmo prazo de recuperação. Stallings (2018) destaca que controles devem ser escolhidos a partir do risco, o que permite concentrar recursos nos componentes mais relevantes.

Assim, mapear criticidade é uma decisão de gestão. A infraestrutura deixa de ser uma coleção de dispositivos e passa a ser compreendida como um conjunto de dependências que sustentam resultados empresariais.

3.2 Análise de impacto, RTO e RPO

O planejamento de recuperação precisa responder a duas perguntas: quanto tempo a organização suporta ficar sem determinado serviço e quanto dado pode perder. Swanson et al. (2010) relacionam essas decisões à análise de impacto e aos objetivos de recuperação.

O Recovery Time Objective representa o período-alvo para restaurar uma função ou sistema. O Recovery Point Objective indica a quantidade de dados, medida no tempo, que a organização admite perder. Embora os conceitos sejam técnicos, sua definição depende de decisões de negócio.

Um RTO muito curto pode exigir redundância, automação e infraestrutura adicional. Um RPO próximo de zero pode demandar replicação frequente ou contínua. Por isso, objetivos de recuperação precisam ser compatíveis com impacto e orçamento.

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: 14/01/2026 | aceito: 17/01/2026 | publicação: 20/01/2026

A ISO 22301 (2019) reforça que continuidade deve ser estruturada em torno das necessidades da organização e de sua capacidade de responder a interrupções. Isso impede que decisões sejam tomadas apenas com base em conveniência técnica.

Também é importante considerar dependências entre sistemas. Restaurar uma aplicação sem banco de dados, autenticação ou conectividade pode não devolver a operação ao usuário. A sequência de recuperação deve refletir essas relações.

RTO e RPO, portanto, funcionam como ponte entre gestão e tecnologia. Quando definidos de maneira realista, orientam backup, redundância, contratos, testes e prioridades de investimento.

3.3 Backup não é sinônimo de recuperação

O backup é um componente da recuperação, mas sua simples existência não garante continuidade. O NIST SP 800-34 Rev. 1 afirma que processos eficazes de backup são cruciais para a estratégia de recuperação e relaciona sua frequência às necessidades identificadas na análise de impacto (SWANSON et al., 2010).

Uma cópia pode falhar por corrupção, configuração incorreta, credenciais comprometidas ou retenção insuficiente. Por isso, a gestão de backup precisa observar cobertura, frequência, integridade, proteção e capacidade de restauração.

Whitman e Mattord (2021) tratam disponibilidade como dimensão central da segurança da informação. Essa perspectiva mostra que proteger dados inclui garantir que possam ser recuperados quando necessários.

A separação lógica ou física de cópias reduz a possibilidade de um único incidente comprometer produção e backup simultaneamente. O desenho adequado depende do ambiente, mas o princípio é evitar pontos únicos de falha.

Políticas de retenção também precisam considerar versões. Uma exclusão acidental ou alteração maliciosa pode ser percebida dias depois; se todas as cópias já refletirem o estado comprometido, o backup perde parte de sua utilidade.

Portanto, a pergunta relevante não é apenas se existe backup, mas se a organização conhece o que está protegido, até quando consegue retornar e quanto tempo levaria para fazê-lo.

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: 14/01/2026 | aceito: 17/01/2026 | publicação: 20/01/2026

3.4 Testes de restauração e capacidade comprovada

Testar recuperação transforma uma expectativa em evidência. Swanson et al. (2010) incluem testes, treinamento e exercícios entre as etapas do planejamento de contingência, justamente porque planos não executados podem conter premissas incorretas.

Um teste de restauração pode revelar arquivos incompletos, dependências esquecidas, senhas indisponíveis ou tempos incompatíveis com o objetivo definido. Esses problemas são menos custosos quando encontrados antes de uma emergência.

A periodicidade deve refletir criticidade e ritmo de mudança. Sistemas modificados com frequência podem exigir validações mais recorrentes. Ambientes estáveis ainda precisam de testes, pois hardware, software, credenciais e pessoas mudam ao longo do tempo.

Exercícios também avaliam comunicação. Recuperação envolve decidir quem autoriza, quem executa, quem valida e quem informa usuários ou clientes. A ISO 22301 (2019) trata a preparação organizacional como parte da continuidade, não apenas a restauração técnica.

O resultado do teste precisa gerar registro. Tempo observado, falhas encontradas, ações corretivas e responsáveis permitem acompanhar evolução e demonstrar que o plano é mantido.

Assim, a capacidade de recuperação é melhor expressa por evidências de testes do que pela quantidade de ferramentas instaladas. Resiliência é uma propriedade operacional comprovada, não uma promessa.

3.5 Documentação e redução da dependência de conhecimento individual

Ambientes de TI acumulam conhecimento informal: endereços, credenciais, regras de firewall, topologias, rotinas e exceções. Quando essas informações ficam concentradas em uma pessoa, a própria equipe se torna um ponto único de falha.

O NIST CSF 2.0 (2024) amplia a ênfase em governança e comunicação de responsabilidades. Documentar ativos, procedimentos e decisões contribui para que a organização consiga manter controles mesmo diante de mudanças de pessoal.

Documentação útil não precisa ser extensa. Inventários atualizados, diagramas de rede, lista de dependências, contatos, procedimentos de recuperação e localização segura de credenciais podem produzir valor maior do que manuais longos e desatualizados.

O controle de versões é igualmente relevante. Um diagrama antigo pode induzir decisões erradas durante um incidente. A documentação deve fazer parte do processo de mudança, e não ser atualizada apenas quando surge uma auditoria ou falha.

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: 14/01/2026 | aceito: 17/01/2026 | publicação: 20/01/2026

Stallings (2018) relaciona políticas e procedimentos à execução consistente da segurança. Em continuidade, a documentação cumpre função semelhante: permite que ações críticas sejam repetidas de forma previsível.

A redução da dependência individual também facilita treinamento e transferência de conhecimento. A resiliência tecnológica, nesse sentido, inclui a capacidade de preservar conhecimento operacional além das pessoas que originalmente configuraram o ambiente.

3.6 Monitoramento, prevenção e ciclo de resiliência

Monitoramento permite identificar degradações antes que se convertam em indisponibilidade percebida pelo usuário. Capacidade de armazenamento, falhas de serviço, perda de conectividade e erros de backup são exemplos de sinais que podem ser acompanhados.

O NIST CSF 2.0 organiza a gestão de risco em Govern, Identify, Protect, Detect, Respond e Recover. Essa estrutura mostra que recuperação não é etapa isolada: ela depende de governança, conhecimento do ambiente, proteção, detecção e resposta coordenadas.

Para PMEs, o valor do monitoramento está na priorização. Alertas excessivos produzem ruído; poucos alertas deixam falhas invisíveis. Criticidade e impacto devem orientar quais eventos exigem ação imediata.

O Verizon DBIR 2025 analisou mais de 22 mil incidentes e 12.195 violações confirmadas, registrando aumento da exploração de vulnerabilidades e participação de terceiros. O cenário reforça a necessidade de combinar disponibilidade e segurança em uma mesma disciplina operacional.

Monitoramento também precisa alcançar o próprio mecanismo de proteção. Uma rotina de backup que deixa de executar deve gerar alerta; caso contrário, a falha pode permanecer invisível até o momento da recuperação.

Resiliência, portanto, é cíclica. Organizações identificam riscos, protegem ativos, detectam desvios, respondem, recuperam e incorporam as lições ao desenho seguinte do ambiente.

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.

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

Ano VII, v.2 2026 | submissão: 14/01/2026 | aceito: 17/01/2026 | publicação: 20/01/2026

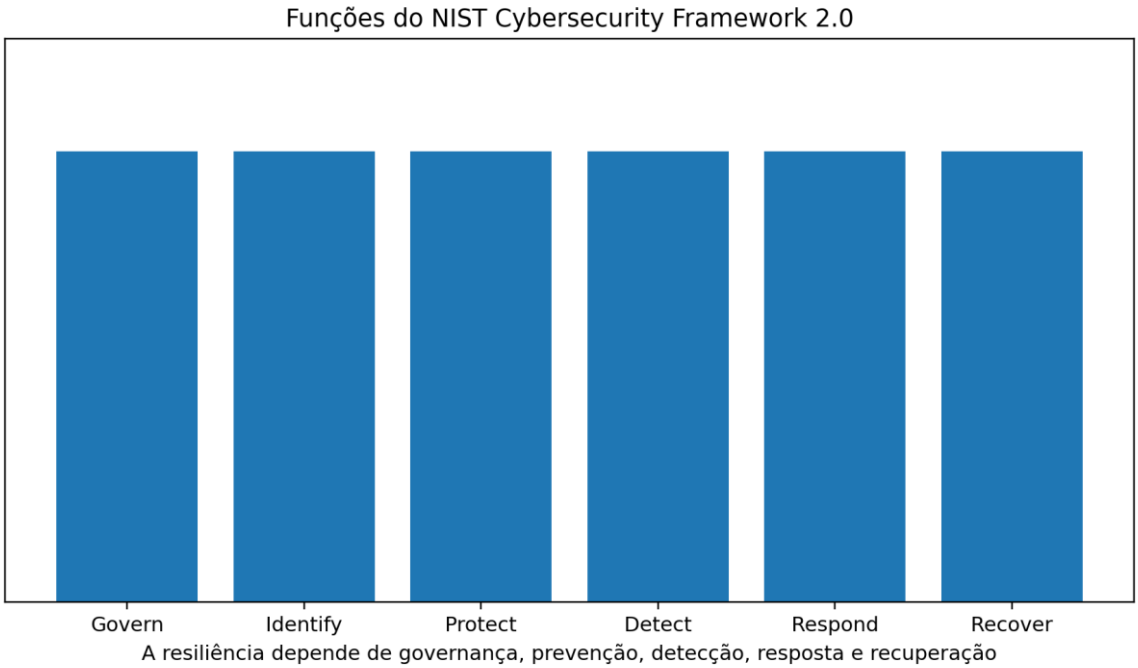


Figura 1. As seis funções do NIST Cybersecurity Framework 2.0. Fonte: elaboração própria com base em Pascoe, Quinn e Scarfone (2024).

3.7 Custo da indisponibilidade e proporcionalidade do investimento

A discussão sobre resiliência também possui dimensão econômica. Investimentos em backup, redundância e segurança competem com outras prioridades, sobretudo em empresas de menor porte. Por isso, a análise não deve partir da ideia de proteção absoluta, mas da comparação entre impacto potencial, probabilidade e custo de controle. O NIST CSF 2.0 (PASCOE; QUINN; SCARFONE, 2024) foi concebido justamente para permitir que organizações priorizem resultados de segurança conforme contexto e risco.

O custo de uma interrupção não se limita à reposição de equipamentos. Horas improdutivas, impossibilidade de faturar, atraso em entregas, recuperação de dados, contratação emergencial de especialistas e perda de confiança podem ampliar o efeito financeiro. Whitman e Mattord (2021) relacionam segurança da informação à continuidade das funções organizacionais, o que reforça a necessidade de observar impactos indiretos.

Em 2025, pesquisa internacional divulgada pela Mastercard com mais de cinco mil proprietários de pequenas e médias empresas em quatro continentes informou que 46% haviam sofrido um ataque cibernético em seu negócio atual. Entre os atingidos, quase um em cada cinco declarou ter posteriormente pedido falência ou encerrado a empresa. O dado não estabelece causalidade

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: 14/01/2026 | aceito: 17/01/2026 | publicação: 20/01/2026

econômica uniforme, mas demonstra a gravidade potencial de incidentes para organizações com menor capacidade de absorção.

A mesma publicação da Mastercard cita estimativa de 2024 segundo a qual o custo médio de um ataque cibernético para empresas com 25 a 299 empregados alcançou US$ 250 mil. Valores dessa natureza não devem ser transplantados automaticamente para qualquer empresa, porque setor, porte e tipo de incidente alteram o impacto. Servem, porém, para demonstrar por que continuidade e segurança também precisam ser avaliadas como decisões financeiras.

A proporcionalidade do investimento exige distinguir controles essenciais de soluções desejáveis. Uma PME pode obter ganhos significativos com inventário confiável, autenticação adequada, cópias protegidas, restauração testada, atualização de sistemas e documentação antes de adotar arquiteturas de alta complexidade. Eliot (2024) reforça essa abordagem ao direcionar o guia do NIST a organizações com planos modestos ou inexistentes.

Desse modo, resiliência tecnológica deve entrar no planejamento empresarial como gestão de exposição. O objetivo econômico não é eliminar todo risco, mas evitar que uma falha previsível produza um impacto desproporcional à capacidade financeira e operacional da organização.

Conclusão

A continuidade tecnológica em pequenas e médias empresas depende menos da quantidade de ferramentas e mais da coerência entre risco, prioridade e capacidade de recuperação.O mapeamento de ativos críticos permite compreender quais dependências sustentam a operação e evita investimentos distribuídos sem critério.A análise de impacto transforma indisponibilidade em parâmetros de decisão. RTO e RPO ajudam a aproximar expectativas empresariais e desenho técnico. Backups são indispensáveis, mas não devem ser confundidos com recuperação. Integridade, retenção, proteção e cobertura precisam ser verificadas.Testes de restauração fornecem a evidência mais concreta de que um plano pode funcionar. Também revelam dependências e tempos que não aparecem em documentos.A documentação reduz o risco de conhecimento concentrado e facilita continuidade diante de mudanças de equipe, fornecedores ou infraestrutura.Monitoramento conecta prevenção e resposta, permitindo que falhas sejam percebidas antes de produzirem impacto maior e que mecanismos de proteção sejam supervisionados.Conclui-se que resiliência tecnológica é uma capacidade organizacional construída continuamente. Para PMEs, soluções proporcionais, documentadas e testadas podem oferecer maior valor do que arquiteturas complexas que não conseguem ser operadas ou recuperadas com segurança.

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: 14/01/2026 | aceito: 17/01/2026 | publicação: 20/01/2026

Referências

PASCOE, Cherilyn; QUINN, Stephen; SCARFONE, Karen. The NIST Cybersecurity Framework (CSF) 2.0. NIST CSWP 29. Gaithersburg: National Institute of Standards and Technology, 2024.
ELIOT, Daniel. NIST Cybersecurity Framework 2.0: Small Business Quick-Start Guide. NIST SP 1300. Gaithersburg: National Institute of Standards and Technology, 2024.
SWANSON, Marianne M.; BOWEN, Pauline; PHILLIPS, Amy W.; GALLUP, Dean; LYNES, David. Contingency Planning Guide for Federal Information Systems. NIST SP 800-34 Rev. 1. Gaithersburg: National Institute of Standards and Technology, 2010.
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). Security and Privacy Controls for Information Systems and Organizations. NIST SP 800-53 Rev. 5. Gaithersburg, 2020.
ISO. ISO 22301:2019 Security and resilience — Business continuity management systems — Requirements. Geneva: International Organization for Standardization, 2019.
VERIZON. 2025 Data Breach Investigations Report. Basking Ridge, 2025.
STALLINGS, William. Effective Cybersecurity: A Guide to Using Best Practices and Standards. Boston: Addison-Wesley, 2018.
WHITMAN, Michael E.; MATTORD, Herbert J. Principles of Information Security. 7. ed. Boston: Cengage, 2021.
MASTERCARD. A small business expert answers your most pressing questions. 2025.

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.