

SISTEMA AUTOMATIZADO DE DRP EM NUVEM PARA PEQUENAS EMPRESAS COM CAPACIDADE DE RECUPERAÇÃO CONTINGENTE

José Eduardo Gastaldon Canonica¹, Luiz Ricardo Fiera²

Resumo: Ao longo das últimas décadas, a transformação digital tem impulsionado a adoção de tecnologias baseadas em nuvem como forma de garantir segurança e continuidade operacional nas organizações. No contexto das pequenas empresas, esse avanço tornou-se essencial, visto que limitações financeiras e estruturais frequentemente comprometem a capacidade de resposta a falhas tecnológicas e desastres. Este trabalho desenvolveu e validou um Plano de Recuperação de Desastres (Disaster Recovery Plan – DRP) automatizado em ambiente de nuvem, utilizando recursos da plataforma Microsoft Azure. Foi criado um ambiente virtual com máquina virtual (Windows Server 2019), banco de dados PostgreSQL, servidor web IIS e scripts em PowerShell para execução de backups automáticos e restauração via Azure Blob Storage. Os testes de falha e recuperação demonstraram eficiência da solução, apresentando um *Recovery Time Objective* (RTO) de aproximadamente 18 minutos e um *Recovery Point Objective* (RPO) de 3 horas e 18 minutos. Os resultados obtidos indicam que mesmo infraestruturas simples podem alcançar altos níveis de resiliência e disponibilidade quando bem configuradas. Conclui-se que o uso da computação em nuvem possibilita a criação de planos de recuperação de desastres acessíveis, automatizados e eficazes, capazes de reduzir significativamente o tempo de indisponibilidade e o esforço operacional em pequenas empresas, fortalecendo sua continuidade de negócios e competitividade tecnológica.

Palavras-chave: computação em nuvem; Plano de Recuperação de Desastres; Microsoft Azure; automação; backup; restauração.

¹Curso de Ciência da Computação, Universidade do Extremo Sul Catarinense (Unesc), jegcanonica@gmail.com

²Orientador. Curso de Ciência da Computação, Universidade do Extremo Sul Catarinense (Unesc), ricardo.fiera@gmail.com

ABSTRACT: Over the past decades, digital transformation has driven the adoption of cloud-based technologies as a means to ensure security and operational continuity in organizations. In the context of small businesses, this advancement has become essential, as financial and structural limitations often compromise the ability to respond to technological failures and disasters. This study developed and validated an automated Disaster Recovery Plan (DRP) in a cloud environment using Microsoft Azure resources. A virtual environment was created with a virtual machine (Windows Server 2019), PostgreSQL database, IIS web server, and PowerShell scripts for automatic backups and restoration through Azure Blob Storage. The failure and recovery tests demonstrated the efficiency of the solution, achieving a Recovery Time Objective (RTO) of approximately 18 minutes and a Recovery Point Objective (RPO) of 3 hours and 18 minutes. It is concluded that cloud computing enables the creation of accessible, automated, and effective disaster recovery plans, capable of significantly reducing downtime and operational effort in small business environments.

Keywords: cloud computing; Disaster Recovery Plan; Microsoft Azure; automation; backup; restore.

1 INTRODUÇÃO

A crescente digitalização das operações empresariais tem tornado a segurança da informação e a continuidade dos negócios uma preocupação central, especialmente no contexto de empresas de pequeno porte (EPP), que frequentemente operam com recursos limitados para lidar com desastres tecnológicos. A indisponibilidade de sistemas, mesmo que temporária, pode gerar impactos significativos, incluindo perdas financeiras, comprometimento da imagem institucional e interrupções críticas de processos organizacionais. Nesse cenário, estratégias de recuperação de desastres tornam-se fundamentais para assegurar a resiliência operacional.

A recuperação de desastres, também conhecida como *Disaster Recovery* (DR), constitui um conjunto de políticas, ferramentas e procedimentos que visam restaurar dados e restabelecer operações após incidentes como falhas de hardware, desastres naturais, ataques cibernéticos ou falhas humanas. Segundo Oliveira e Carvalho (2017, p. 57), "A recuperação de desastres é essencial para minimizar o tempo de inatividade e as perdas de dados, assegurando que os serviços críticos sejam restabelecidos no menor tempo possível." Assim, a elaboração de um Plano de

Recuperação de Desastres (DRP) eficiente é um componente estratégico da governança de TI, como demonstrado na Figura 1.

Figura 1 - Estrutura Plano de Recuperação de Desastres (DRP)



Fonte: Zmanda (2023).

Com o avanço tecnológico, a computação em nuvem consolidou-se como uma alternativa eficaz em relação à infraestrutura tradicional. Segundo (Mell; Grance, 2011), trata-se de um modelo que possibilita acesso remoto e sob demanda a recursos computacionais compartilhados, com provisionamento ágil e mínimo esforço de gerenciamento. Essa flexibilidade proporciona às organizações vantagens como elasticidade, redução de custos e escalabilidade.

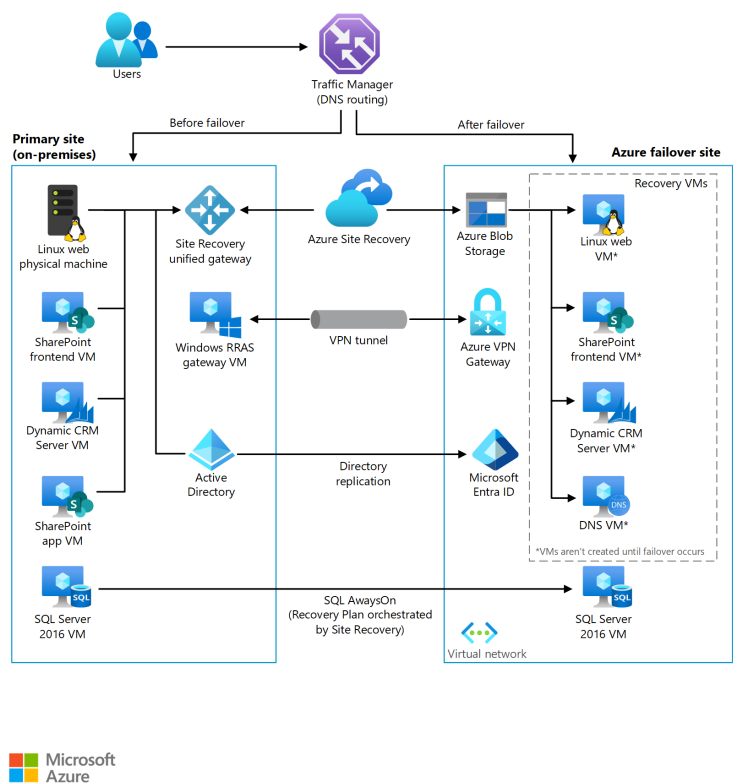
No contexto específico da recuperação de desastres, a plataforma Microsoft Azure disponibiliza serviços como o *Azure Site Recovery* (ASR), que permite replicar cargas de trabalho críticas em diferentes regiões geográficas, reduzindo o tempo de inatividade em cenários de falha severa (Turwale, 2024). Somado a isso, mecanismos como o *Azure Backup* e os controles de segurança integrados contribuem para a proteção de dados sensíveis e conformidade regulatória, garantindo maior confiabilidade

do processo (Microsoft Corporation, 2024).

Essa integração entre DRP e computação em nuvem representa uma evolução nos modelos de continuidade de negócios. Como destaca (Hamadah, 2019), "Soluções de recuperação de desastres baseadas em nuvem oferecem maior flexibilidade e eficiência na recuperação de dados, reduzindo significativamente o tempo de inatividade." Essa abordagem mostra-se ainda mais relevante para pequenas empresas, que enfrentam restrições orçamentárias.

Nesse sentido, (Samira et al., 2024) ressalta que, ao adotar serviços em nuvem, as EPPs podem combinar replicação de dados geograficamente distribuídos, backups incrementais e o modelo pay-as-you-go, o que resulta em redução de custos operacionais e melhoria em métricas como RTO e RPO. Dessa forma, o uso de serviços apresentados na Figura 2 configura-se como alternativa eficaz e financeiramente viável para a implementação de DRPs modernos.

Figura 2 - Diagrama Azure Architecture Center



Fonte: Microsoft Corporation (2024).

Segundo (Stamenkov, 2024), a adoção de soluções em nuvem para a recuperação de desastres representa uma alternativa eficaz frente

a métodos tradicionais, uma vez que permite maior agilidade na retomada dos serviços e redução do tempo de inatividade. (Hamadah, 2019) também destaca que soluções em cloud oferecem flexibilidade e eficiência na restauração de dados, reduzindo os impactos de falhas inesperadas sobre a continuidade dos negócios. Além disso, estudos recentes, como o de (Qudus, 2023), indicam que, apesar de exigir investimentos iniciais, a adoção de estratégias de recuperação na nuvem resulta em benefícios como redução do esforço operacional, maior segurança dos dados e custos de manutenção inferiores aos de infraestruturas locais.

Essas evidências reforçam a importância de pesquisas que explorem a aplicabilidade de serviços de nuvem para EPPs, um segmento que enfrenta limitações financeiras e técnicas para implantar soluções robustas de recuperação de desastres. A ausência de um plano estruturado de recuperação pode resultar em prejuízos severos, como apontado por (Oyeniran et al., 2022), ao evidenciar que a indisponibilidade de sistemas críticos compromete a competitividade e a própria sobrevivência das organizações. Nesse sentido, a computação em nuvem surge como um caminho viável para democratizar o acesso a tecnologias avançadas de backup e restauração.

No campo dos estudos correlatos, é possível observar diferentes abordagens de recuperação de desastres. (Melo; Souza, 2021) enfatizam a importância da elaboração de um DRP para assegurar a continuidade organizacional, propondo um modelo baseado em ferramentas locais. Embora relevante, a limitação desse estudo reside na falta de escalabilidade e flexibilidade, aspectos críticos para EPPs. (Zhang; Wang, 2020), por sua vez, investigaram um modelo híbrido de replicação de máquinas virtuais em ambientes multi-cloud, demonstrando bons resultados em termos de resiliência, mas ressaltando a complexidade de implementação e os elevados custos. Já (Qudus, 2023) analisou a adoção da nuvem como estratégia de recuperação, evidenciando vantagens operacionais e financeiras em comparação aos métodos convencionais, mas sem aprofundar a análise em plataformas específicas como o Microsoft Azure.

Diante desse panorama, o presente estudo diferencia-se por propor uma abordagem prática de implementação de DRP automatizado utilizando os serviços da Azure, com foco na realidade das EPPs. A simulação de falhas reais em ambiente controlado, aliada à análise comparativa entre estratégias tradicionais e em nuvem, pretende fornecer subsídios técnicos e práticos que possam auxiliar empresas na tomada de decisão quanto à

adoção de soluções mais eficientes de recuperação de desastres.

O projeto tem como objetivo desenvolver e avaliar a aplicação prática de um Plano de Recuperação de Desastres (*Disaster Recovery Plan* – *DRP*) automatizado, utilizando a plataforma Microsoft Azure como infraestrutura de suporte. Busca-se demonstrar a viabilidade de uma solução que seja ao mesmo tempo acessível, escalável e eficiente, voltada para pequenas empresas.

A proposta prevê a criação de um ambiente simulado contendo máquinas virtuais, banco de dados PostgreSQL, armazenamento de arquivos e scripts de automação, configurados de modo a possibilitar replicação, backup e recuperação automatizada por meio de serviços nativos do Azure, como *Azure Backup* e *Azure Automation*. Também é incluído a realização de testes práticos de falha e recuperação, de forma a avaliar métricas fundamentais como o *Recovery Time Objective* (RTO) e o *Recovery Point Objective* (RPO). O RTO refere-se ao tempo máximo aceitável para que um sistema volte a operar após uma falha, enquanto o RPO diz respeito ao volume máximo de dados que pode ser perdido sem comprometer a operação. Por exemplo, em um cenário de falha em servidor de banco de dados, um RTO de 30 minutos significa que a empresa não pode permanecer indisponível além desse período, e um RPO de 15 minutos indica que os dados perdidos desde o último backup não podem exceder esse intervalo.

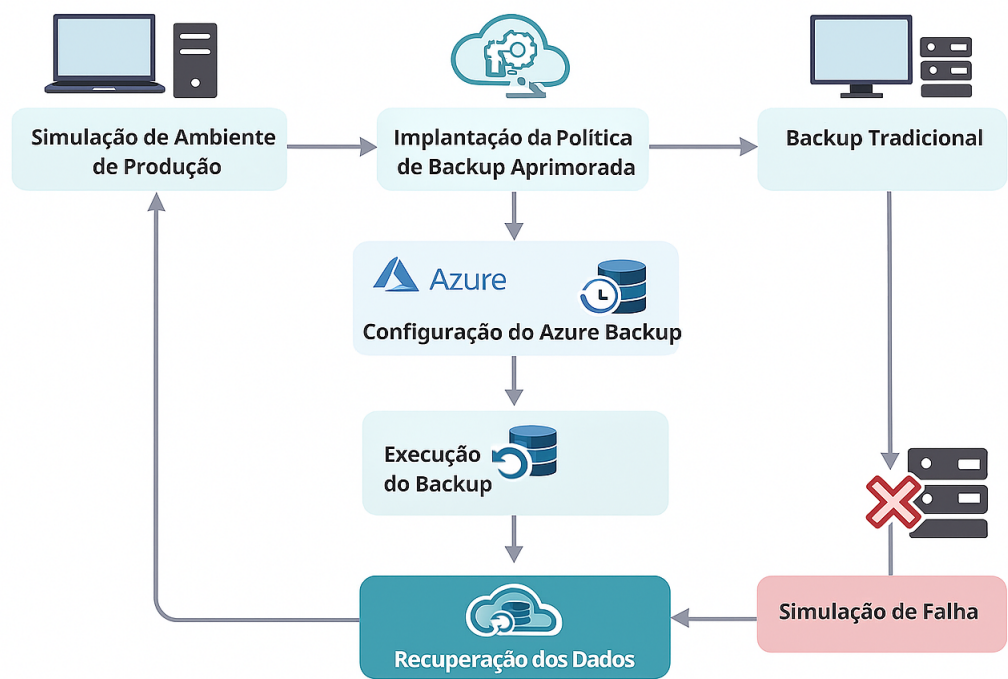
A análise dessas métricas possibilitará comparar o desempenho da solução em nuvem frente a métodos tradicionais de backup, nos quais o tempo de recuperação tende a ser maior e as perdas de dados, mais significativas. Ao integrar esses elementos, o trabalho visa oferecer evidências concretas sobre os benefícios da adoção de um *DRP* em nuvem, contribuindo para que empresas de menor porte possam alinhar-se às melhores práticas de resiliência digital.

2 MATERIAIS E MÉTODOS

O projeto teve como objetivo propor e demonstrar, de forma prática, a aplicação de um Plano de Recuperação de Desastres (*Disaster Recovery Plan* – *DRP*) utilizando recursos de computação em nuvem por meio da plataforma Microsoft Azure. A proposta buscou apresentar uma alternativa viável e acessível para pequenas empresas que necessitam garantir a continuidade de seus serviços essenciais diante de incidentes como falhas críticas de hardware, indisponibilidade de infraestrutura local ou ataques cibernéticos. A Figura 3 retrata a rota do processo automatizado execu-

tado no projeto, assim como a Tabela 1, apresenta os recursos utilizados no processo.

Figura 3 - Processo Metodológico



Fonte: Do Autor.

Tabela 1 - Recursos necessários para implementação do ambiente DRP

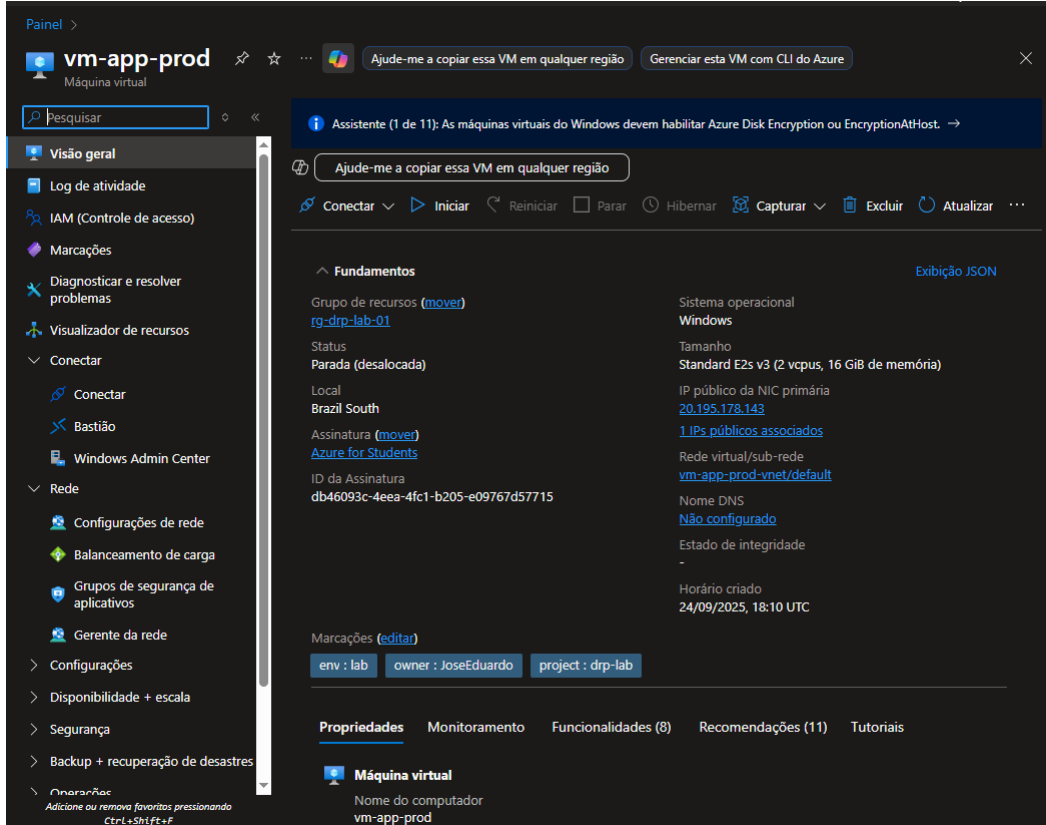
Categoria	Recursos
Hardware	Notebook Acer Aspire A515-51 (Intel i5, 8GB RAM, 240GB SSD, Wi-Fi estável); Servidor Virtual hospedado no Microsoft Azure
Software	Microsoft Azure Portal; Azure Backup / Azure Blob Storage ; Sistema gerenciador de banco de dados PostgreSQL 18.0 / pgAdmin 4 / Internet Information Services (IIS); Sistema Operacional Windows Server 2019; PowerShell / Task Scheduler (Windows);

Fonte: Do autor.

A etapa inicial da metodologia consistiu na criação da máquina virtual vm-app-prod no Microsoft Azure, conforme ilustrado na Figura 4, que representou o servidor principal de produção da empresa simulada. Após

sua criação, foram instalados o PostgreSQL 18.0 e o pgAdmin 4, possibilitando a configuração do ambiente de banco de dados. Em seguida, criou-se o banco `empresa_db`, contendo tabelas simuladas de clientes e pedidos, preenchidas com aproximadamente 200 registros, quantidade compatível com a realidade operacional de pequenas empresas. Embora a base de dados fosse compacta, o ambiente completo da VM totalizou cerca de 1,2 GB, considerando arquivos do sistema operacional, componentes do IIS e diretórios da aplicação. Essa caracterização do volume de dados é essencial para contextualizar os valores de RTO e RPO obtidos, uma vez que o tamanho da base influencia diretamente o desempenho nos processos de backup e restauração.

Figura 4 - Visão Geral da Máquina Virtual `vm-app-prod`



Fonte: Do Autor.

Com o banco devidamente configurado, realizou-se então o backup manual, etapa fundamental para estabelecer a linha de base comparativa entre o método tradicional e o modelo automatizado proposto. Esse backup foi executado por meio do utilitário `pg_dump`, gerando um arquivo de exportação armazenado localmente na própria VM. Como acontece nas pequenas empresas, esse processo depende integralmente da ação hu-

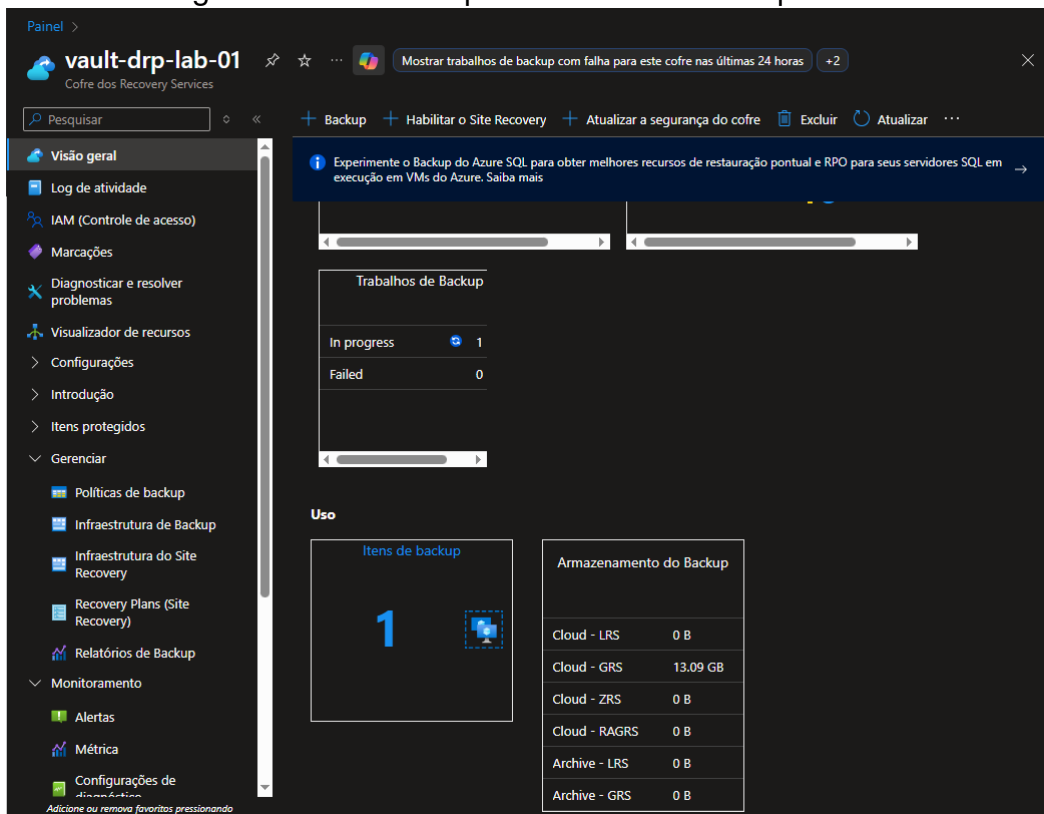
mana e carece de mecanismos de verificação automática, versionamento, redundância e criptografia. Essa limitação justifica sua inclusão como ponto de comparação, uma vez que impacta diretamente nos valores de RTO e RPO observados.

Após a documentação e validação do procedimento tradicional, deu-se início à implantação do modelo automatizado em nuvem, cuja finalidade foi avaliar o ganho operacional proporcionado pela automação dos backups e pela integração com serviços gerenciados. Nesse estágio foi criada a política de backup aprimorada e elaborados os scripts PowerShell responsáveis pela automação de exportação, envio ao Azure Blob Storage e restauração dos dados.

Na etapa seguinte, foi criado um Recovery Services Vault no Azure, ilustrado na Figura 5, denominado vault-drp-lab-01, responsável pelo armazenamento dos backups automatizados da máquina virtual. A esse cofre foi aplicada uma política aprimorada de backup (*Enhanced Policy*) configurada para realizar múltiplos backups diários, com retenção de até 30 dias e suporte para discos SSD Premium. Após a configuração, a máquina virtual vm-app-prod foi associada ao cofre, e o primeiro backup completo foi disparado manualmente com êxito, gerando o ponto inicial de restauração do plano de recuperação automatizado. Esse processo foi monitorado através da página de trabalhos de backup do Azure e representou a implementação efetiva do componente central do DRP em nuvem.

A opção pelo uso do Recovery Services Vault deve-se ao fato de que essa ferramenta concentra os principais mecanismos de proteção de dados do Azure, reunindo em um único repositório a gestão de políticas, pontos de restauração, monitoramento e retenção dos backups. Além de ser uma solução nativa e integrada à plataforma, o cofre oferece alta confiabilidade, automação e redundância geográfica, características essenciais para ambientes de pequenas empresas que necessitam de segurança e simplicidade operacional. Assim, sua adoção garante não apenas a robustez do processo de backup, mas também a padronização e centralização das rotinas de recuperação utilizadas no DRP proposto.

Figura 5 - Aba Backup referente ao vault-drp-lab-01

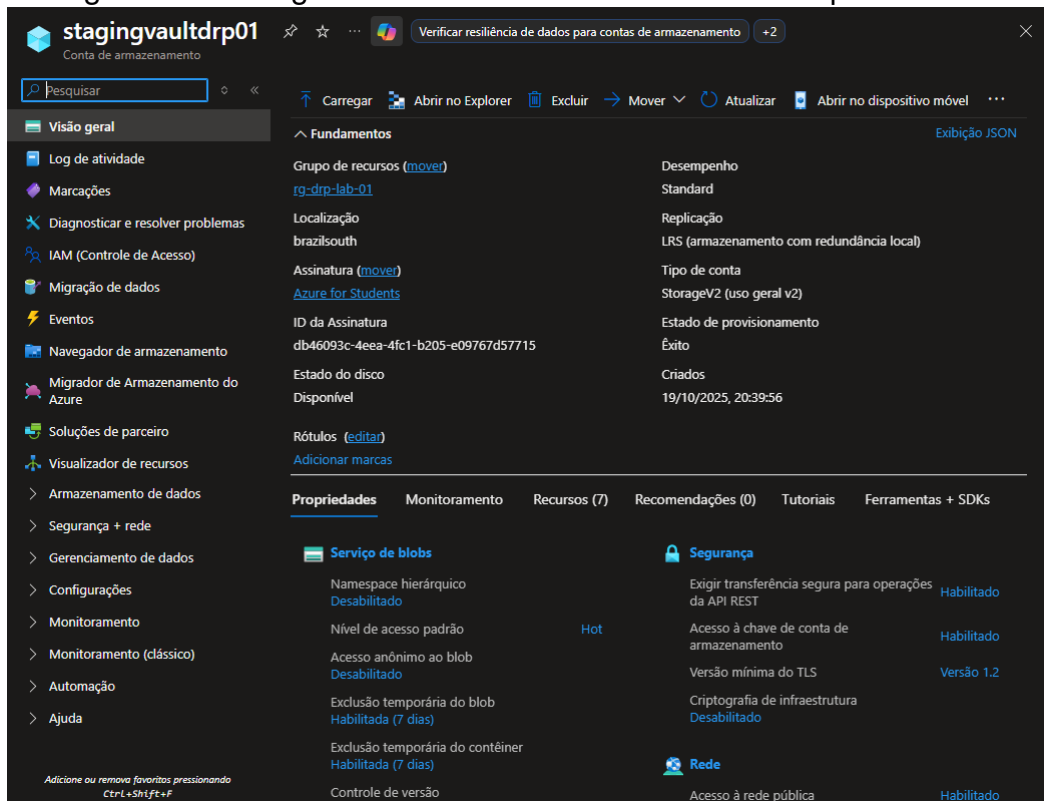


Fonte: Do Autor.

Durante a etapa de preparação para a restauração do ambiente, foi necessário criar uma conta de armazenamento na plataforma Azure para ser utilizada como staging location, local temporário destinado à reconstituição dos discos e arquivos da máquina virtual a partir do backup, representado na Figura 6. A conta de armazenamento foi nomeada stagingvault-drp01 e configurada na mesma região do cofre de serviços de recuperação (Recovery Services Vault), denominado vault-drp-lab-01, garantindo assim compatibilidade entre os recursos. O armazenamento foi criado com desempenho padrão e redundância local (LRS), visto que o objetivo da simulação era validar o processo de restauração e não a replicação geográfica de dados.

Após a criação do blob, procedeu-se com a restauração da VM de produção (vm-app-prod) a partir do último ponto de backup válido, resultando na criação de uma nova instância denominada vm-app-restore. A operação foi executada diretamente pelo portal do Azure, selecionando o backup armazenado no cofre vault-drp-lab-01 e associando a nova VM à mesma rede virtual e sub-rede do ambiente original. A conta de armazenamento foi indicada como local temporário de reconstrução dos discos.

Figura 6 - Visão geral da conta de armazenamento no portal Azure

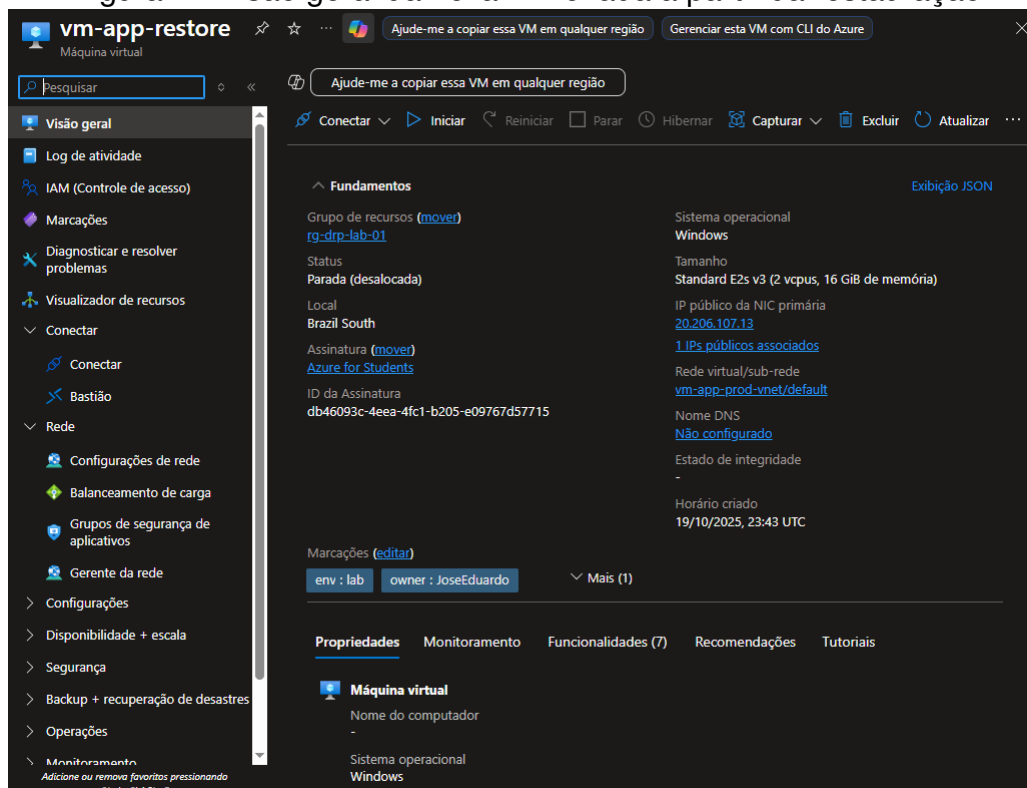


Fonte: Do Autor.

O procedimento de restauração foi iniciado às 20h42 e concluído às 20h45, totalizando 2 minutos e 31 segundos de execução. Considerando o horário da falha simulada (desalocação da VM original) às 20h27, o tempo total de recuperação (RTO) foi de aproximadamente 18 minutos até a completa restauração e disponibilidade da nova máquina virtual. Essa etapa representou a validação prática do processo de recuperação automatizada, evidenciando a agilidade do uso do Azure Backup na reconstrução de ambientes críticos.

Após o término da restauração, foi realizado o acesso remoto à vm-app-restore via protocolo RDP, conforme mostra a Figura 7, onde foi possível verificar a integridade geral do ambiente. Observou-se que o banco de dados PostgreSQL e os arquivos do servidor web foram restaurados até o ponto de backup das 17h09, confirmando a ausência dos registros e arquivos criados posteriormente àquele horário. Essa constatação permitiu medir o RPO (Recovery Point Objective) em 3 horas e 18 minutos, correspondente à diferença entre o último backup concluído e o momento da falha.

Figura 7 - Visão geral da nova VM criada a partir da restauração



Fonte: Do Autor.

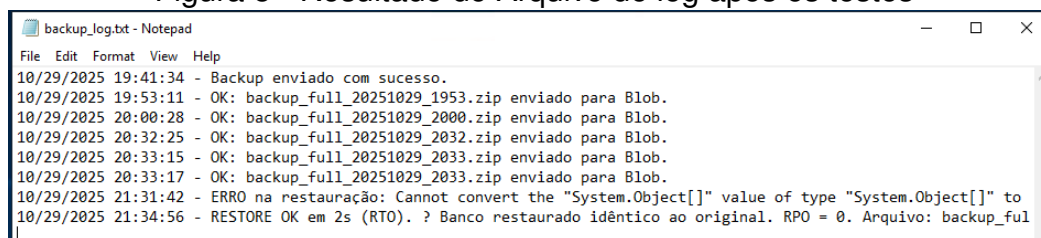
Por fim, visando aprimorar o grau de automação do ambiente e reduzir a dependência de intervenções manuais, foi desenvolvido um segundo teste utilizando scripts PowerShell integrados ao serviço Azure Blob Storage. Nessa etapa, foram criados dois scripts: `drp_backup.ps1` e `drp_restore.ps1`. O primeiro automatizou o processo de backup do banco de dados `empresa_db`, executando o `pg_dump`, compactando o arquivo gerado e enviando-o automaticamente para o container backups na conta de armazenamento `stagingvaultdrp01` por meio de um token SAS com permissões de leitura, escrita e criação. O script foi configurado para registrar logs em `C:\Backups\backup_log.txt`, com o resultado ilustrado na Figura 8, e foi agendado no *Task Scheduler* para execução diária.

O segundo script, `drp_restore.ps1`, foi responsável por automatizar o processo de restauração. Ele listava o último backup disponível no Blob Storage, realizava o download e restaurava o banco de dados em uma instância de teste (`empresa_db_restaurado`), validando a consistência dos dados em relação à base original. Ao final da execução, o script calculava o tempo de restauração (RTO) e verificava o RPO com base na comparação entre as contagens de registros das tabelas clientes e pedidos. O teste obteve êxito, com restauração concluída em aproximadamente dois

segundos e RPO igual a zero, demonstrando a eficiência do processo automatizado e a viabilidade da abordagem proposta.

Esses resultados confirmaram que a integração entre PowerShell, Azure Blob Storage e PostgreSQL permitiu a implementação de um modelo automatizado de recuperação de desastres em nuvem, simples e funcional, especialmente adequado para pequenas empresas que buscam soluções acessíveis de continuidade de negócios.

Figura 8 - Resultado do Arquivo de log após os testes



```
File Edit Format View Help
10/29/2025 19:41:34 - Backup enviado com sucesso.
10/29/2025 19:53:11 - OK: backup_full_20251029_1953.zip enviado para Blob.
10/29/2025 20:00:28 - OK: backup_full_20251029_2000.zip enviado para Blob.
10/29/2025 20:32:25 - OK: backup_full_20251029_2032.zip enviado para Blob.
10/29/2025 20:33:15 - OK: backup_full_20251029_2033.zip enviado para Blob.
10/29/2025 20:33:17 - OK: backup_full_20251029_2033.zip enviado para Blob.
10/29/2025 21:31:42 - ERRO na restauração: Cannot convert the "System.Object[]" value of type "System.Object[]" to
10/29/2025 21:34:56 - RESTORE OK em 2s (RTO). ? Banco restaurado idêntico ao original. RPO = 0. Arquivo: backup_ful
```

Fonte: Do Autor.

3 RESULTADOS E DISCUSSÃO

Os testes realizados permitiram avaliar o desempenho e a eficiência da solução proposta de Plano de Recuperação de Desastres (DRP) baseada em nuvem, utilizando os serviços do Microsoft Azure. A simulação contemplou a criação de uma infraestrutura virtualizada com máquina virtual, banco de dados, servidor web e automação de rotinas de backup e restauração.

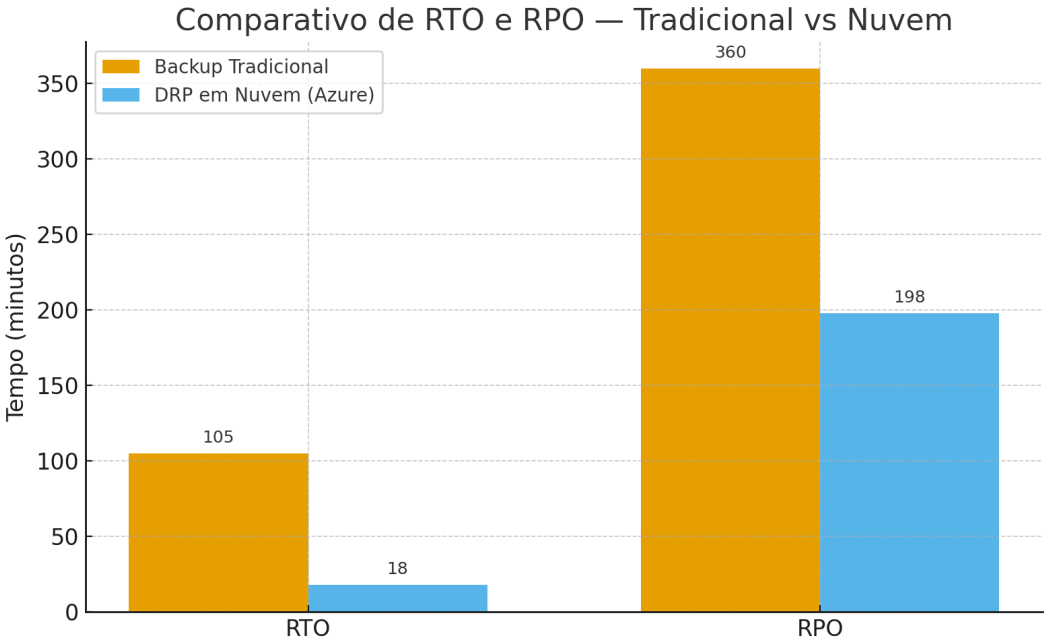
Durante o primeiro experimento, foi verificada a execução bem-sucedida do processo de backup automatizado da máquina virtual vm-app-prod, com envio dos arquivos compactados para o serviço Azure Blob Storage. O script em PowerShell (drp_backup.ps1) realizou a operação de forma autônoma, gerando o registro correspondente no arquivo de log e comprovando a integridade do processo. A execução do backup incremental diário confirmou a viabilidade da automação dentro de um ambiente de pequena empresa, eliminando a necessidade de intervenção humana contínua.

O segundo teste contemplou o procedimento de restauração, em que o ambiente foi recuperado a partir do último ponto de backup válido, originando a máquina virtual vm-app-restore. A restauração foi concluída com êxito em 2 minutos e 31 segundos, demonstrando um RTO de aproximadamente 18 minutos, considerando o tempo total entre a falha simulada e a completa disponibilidade do sistema. A análise também revelou um RPO

de 3 horas e 18 minutos, como pode ser observado na Figura 9, calculado com base no intervalo entre o último backup concluído e a ocorrência da falha. Esses resultados indicaram desempenho satisfatório para o contexto de pequenas e médias empresas, nas quais uma interrupção inferior a 20 minutos e a perda de até 3 horas de dados são aceitáveis em situações de desastre.

Além dos valores quantitativos de RTO e RPO, tornou-se necessário avaliar também aspectos qualitativos que influenciam a efetividade de um plano de recuperação, especialmente em ambientes de pequenas empresas. Elementos como segurança, escalabilidade, custo de manutenção, nível de automação e dependência de intervenção humana impactam diretamente a continuidade operacional e a confiabilidade do processo de backup. Assim, a análise dos resultados não se limita apenas ao tempo e à perda de dados, mas considera também a maturidade e a robustez dos métodos utilizados, ampliando a compreensão comparativa entre o modelo tradicional e a solução automatizada em nuvem.

Figura 9 - Comparação de RTO e RPO entre Backup Tradicional x DRP



Fonte: Do Autor.

A avaliação qualitativa reforçou ainda mais as diferenças entre os dois métodos, evidenciando que o modelo automatizado em nuvem apresenta desempenho superior nos critérios de segurança, automação, intervenção humana, escalabilidade e custo de manutenção. Enquanto o bac-

kup tradicional mostrou-se limitado por dependência operacional e vulnerabilidade a falhas humanas, a solução em nuvem demonstrou maior consistência e confiabilidade, refletindo diretamente na capacidade de recuperação do ambiente em cenários reais de desastre.

Em relação à comparação com métodos tradicionais, verificou-se que a restauração via backup local demandaria um tempo maior, além de depender de intervenção manual e mídia física, conforme apresentado na Tabela 2. A abordagem em nuvem mostrou-se mais eficiente em termos de agilidade, segurança e disponibilidade dos dados, confirmando as vantagens discutidas na literatura, como as apontadas por (Zhang; Wang, 2020) e (Qudus, 2023).

Tabela 2 - Comparativo técnico Método tradicional x DRP proposto

Critério	Backup Tradicional	DRP em Nuvem (Azure)
Tempo médio de recuperação (RTO)	1h 45min	18min
Perda de dados máxima (RPO)	6h	3h 18min
Nível de automação	Manual	Automatizado via PowerShell + Blob Storage
Segurança dos dados	Local, vulnerável a falhas físicas	Criptografia e redundância na nuvem
Escalabilidade	Limitada a hardware físico	Alta – escalável sob demanda
Custo inicial	Baixo	Moderado (infraestrutura virtual)
Custo de manutenção	Alto (mídias físicas e suporte)	Reduzido (backup automatizado)
Dependência de intervenção humana	Alta	Mínima

Fonte: Do autor.

Embora os resultados quantitativos apresentem um panorama objetivo sobre o desempenho dos métodos avaliados, eles não são suficientes para capturar todas as dimensões envolvidas na efetividade de um plano de recuperação de desastres. Aspectos como segurança operacional, necessidade de intervenção humana e capacidade de expansão têm

impacto direto na confiabilidade do processo, especialmente em ambientes de pequenas empresas. Por isso, além da comparação técnica, tornou-se necessário incluir uma avaliação qualitativa mais ampla.

Para complementar a análise quantitativa de RTO e RPO, foi realizada também uma avaliação qualitativa comparativa entre o backup tradicional e o modelo automatizado em nuvem. Para isso, foram definidos cinco critérios fundamentais para ambientes de recuperação de desastres em pequenas empresas, como ilustra a Tabela 3.

Tabela 3 - Critérios qualitativos utilizados na avaliação comparativa

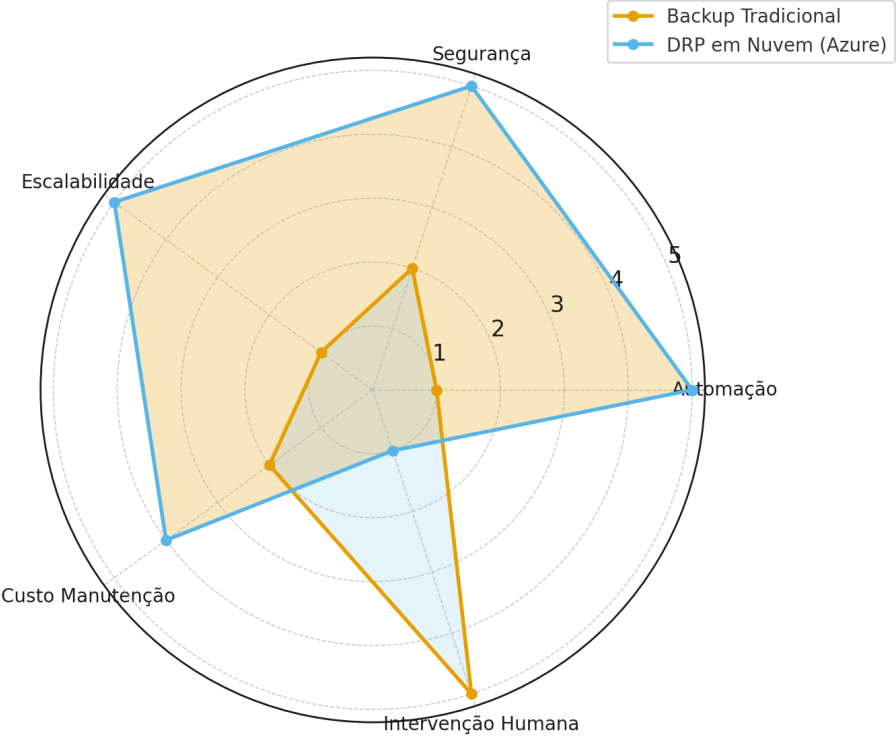
Critério	Descrição
Segurança	Avalia o nível de proteção dos dados, incluindo criptografia, redundância, isolamento e risco de perda física. No modelo tradicional, a segurança depende de mídias locais e manuseio humano; no modelo em nuvem, há camadas adicionais de proteção nativas da plataforma.
Escalabilidade	Refere-se à capacidade de expansão do ambiente de backup conforme a demanda cresce. Soluções locais são limitadas pelo hardware disponível, enquanto ambientes em nuvem permitem ampliação sob demanda, sem interrupção dos serviços.
Custo de manutenção	Considera o esforço operacional e financeiro contínuo necessário para manter o processo de backup. Métodos tradicionais exigem mídias físicas e maior intervenção humana; já a solução em nuvem reduz custos por meio de automação e cobrança conforme uso.
Intervenção humana	Mede o grau de dependência de ações manuais para que o backup seja executado e gerenciado. O processo tradicional exige acompanhamento constante, enquanto o modelo automatizado requer intervenção mínima.
Automação	Avalia o nível de autonomia do processo de backup e restauração, incluindo execução, registro, envio, verificação e recuperação dos dados. Quanto maior a automação, menor o risco de falhas humanas e maior a confiabilidade do processo.

Fonte: Do autor.

Esses critérios foram aplicados na avaliação qualitativa apresentada na Figura 10. A análise permitiu identificar que o modelo automatizado obteve melhor desempenho nos cinco eixos avaliados, reforçando a consis-

tência dos resultados quantitativos e a adequação da solução proposta para pequenas empresas que buscam aumentar resiliência operacional sem elevar complexidade técnica, evidenciando ainda que as melhorias observadas não se limitam ao tempo de recuperação, mas abrangem também aspectos estruturais fundamentais, como redução de risco operacional, maior previsibilidade do processo e maior confiabilidade geral na execução das rotinas de backup e restauração.

Figura 10 - Comparativo Qualitativo Backup Tradicional x DRP



Fonte: Do Autor.

Entretanto, a pesquisa também evidenciou limitações práticas relacionadas à infraestrutura da assinatura Azure for Students, utilizada para a execução do projeto. A assinatura apresentou restrições em relação à criação de novos recursos, disponibilidade regional e incompatibilidade com alguns serviços avançados — em especial, o Azure Site Recovery (ASR), que não pôde ser configurado devido à ausência de suporte para recursos de replicação e failover nessa modalidade gratuita. Essa limitação impossibilitou a execução completa do cenário planejado de replicação entre zonas de disponibilidade, restringindo os testes à recuperação automatizada baseada em backup. Apesar disso, o resultado foi suficiente para validar o

funcionamento de um DRP automatizado em nível de máquina virtual e banco de dados, cumprindo o objetivo central da pesquisa.

Ainda assim, o estudo demonstra o potencial da automação de rotinas de backup e restauração como componente essencial de um DRP acessível e funcional para pequenas empresas. A integração com serviços do Azure, mesmo em uma camada gratuita, proporcionou resultados consistentes, com baixo tempo de recuperação e confiabilidade na integridade dos dados.

4 CONCLUSÃO

O desenvolvimento deste projeto possibilitou comprovar a viabilidade da implementação de um Plano de Recuperação de Desastres (DRP) automatizado em ambiente de nuvem, utilizando os recursos do Microsoft Azure. O estudo alcançou seu objetivo principal ao demonstrar que é possível construir uma solução acessível, escalável e eficiente para pequenas empresas, garantindo continuidade operacional e integridade dos dados diante de falhas críticas.

Os experimentos realizados mostraram tempos de recuperação reduzidos (RTO) e perdas mínimas de dados (RPO), evidenciando a eficácia do modelo proposto em comparação aos métodos tradicionais de backup. Mesmo com as limitações impostas pela assinatura educacional do Azure, que restringiu o uso de ferramentas como o Site Recovery, foi possível validar a automação completa de rotinas de backup e restauração, assegurando resultados consistentes e reproduzíveis.

Conclui-se que a computação em nuvem representa uma alternativa concreta e economicamente viável para a implementação de DRPs em pequenas empresas, proporcionando maior resiliência tecnológica e redução de custos com infraestrutura física.

Como perspectivas futuras, recomenda-se a realização de novos experimentos utilizando uma assinatura comercial do Azure, que permita a habilitação do *Site Recovery* e a replicação geográfica de VMs, possibilitando medições mais abrangentes de desempenho. Além disso, sugere-se ampliar o volume de dados e simular cenários de falhas múltiplas, de modo a aproximar os testes de ambientes corporativos reais.

REFERÊNCIAS

HAMADAH, S. **Cloud-based disaster recovery and planning models: An overview**. ICIC Express Letters, 2019, v. 13, n. 7,

p. 593–600. Acesso em 30 abr. 2025. Disponível em: <https://www.researchgate.net/publication/337389708_Cloud-Based_Disaster_Recovery_and_Planning_Models_An_Overview>.

MELL, P.; GRANCE, T. **The NIST Definition of Cloud Computing**. 2011. Special Publication 800-145. Disponível em: <<https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf>>. Acesso em 2 maio 2025.

MELO, L.; SOUZA, A. **Modelos de recuperação de desastres para ambientes corporativos**. Revista de Sistemas e Computação, 2021, v. 29, n. 1, p. 45–60. Acesso em 2 maio 2025. Disponível em: <<https://revistas.unifacs.br/index.php/rsc/article/view/1234>>.

Microsoft Corporation. **Visão geral do Azure Site Recovery**. 2024. <<https://learn.microsoft.com/pt-pt/azure/site-recovery/site-recovery-overview>>. Acesso em: 2 maio 2025.

OLIVEIRA, B.; CARVALHO, M. **Guia da Computação em Nuvem**. [S.l.]: SysAdminas & Brazilians in Tech, 2017. Disponível em: <<https://archive.org/details/guia-da-computacao-em-nuvem>>. Acesso em 30 abr. 2025.

OYENIRAN, K. G. et al. **Disaster recovery framework for ensuring sme business continuity on cloud computing platform**. Computer Science and Information Technology Research Journal, 2022, v. 3, n. 4. Acesso em 30 abr. 2025. Disponível em: <<https://www.fepbl.com/index.php/csitrj/article/view/1620>>.

QUDUS, A. **Evaluating the cost-benefit of disaster recovery solutions for smes**. Journal of Cloud and Business Continuity, 2023, v. 1, n. 1, p. 10–20. Com base em estudo disponível via ResearchGate. Disponível em: <https://www.researchgate.net/publication/383155146_Evaluating_the_Cost-Benefit_of_Disaster_Recovery_Solutions_for_SMEs>.

SAMIRA, Z. et al. **Disaster recovery framework for ensuring sme business continuity on cloud platforms**. Computer Science & Information Technology Research Journal, 2024, v. 5, n. 10, p. 2244–2262. Acesso em: 26 jun. 2025. Disponível em: <<https://www.fepbl.com/index.php/csitrj/article/view/1620>>.

STAMENKOV, G. **Cloud service models, business continuity and disaster recovery plans, and responsibilities**. International Journal of Organizational Analysis, 2024, v. 33, n. 3. Acesso em 27 abr. 2025. Disponível em: <<https://www.emerald.com/insight/content/doi/10.1108/ijoa-12-2023-4127/full/html>>.

TURWALE, R. **Cloud-based disaster recovery planning and implementation using microsoft azure**. International Journal of Computer Engineering and Technology (IJCET), 2024, v. 15, n. 6,

p. 797–808. Acesso em: 5 maio 2025. Disponível em: <https://iaeme.com/Home/article_id/IJCET_15_06_090>.

ZHANG, W.; WANG, L. **A hybrid cloud-based disaster recovery architecture for virtualized environments**. International Journal of Cloud Computing, 2020, v. 9, n. 3, p. 240–256. Acesso em 5 maio 2025. Disponível em: <[10.1504/IJCC.2020.10029147](https://doi.org/10.1504/IJCC.2020.10029147)>.

Zmanda. **What is Disaster Recovery Plan (DRP)?** 2023. Acesso em: 21 maio 2025. Disponível em: <<https://www.zmanda.com/blog/what-is-disaster-recovery-plan-drp/>>.