DESENVOLVIMENTO DE UM PROCESSO DE RECUPERAÇÃO DE DESASTRES (DISASTER RECOVERY) APLICADO A SEGURANÇA DE DADOS EMPRESARIAIS

Mateus Brognoli Silvano [1], Gustavo Bisognin [2]

Resumo: A Recuperação de Desastres (Disaster Recovery) em sistemas de Tecnologia da Informação, destaca a importância de assegurar a continuidade das operações e a recuperação ágil de dados e infraestrutura em situações adversas, como falhas de hardware ou ataques cibernéticos. A dificuldade reside em criar estratégias eficientes que reduzam prejuízos e possibilitem a retomada das atividades. Elementos fundamentais englobam a identificação de riscos, elaboração de planos de contingência, aplicação de soluções tecnológicas e testes constantes. A distribuição correta de recursos é crucial para o êxito dessas estratégias. O estudo sugere um procedimento para a recuperação de desastres, com ênfase na proteção de dados corporativos, testado em uma rede de supermercados, com o objetivo de assegurar a proteção de ativos vitais.

Palavras-chave: Recuperação de Desastres; Tecnologia da informação, Infraestrutura.

ABSTRACT: Disaster Recovery in Information Technology systems highlights the importance of ensuring operational continuity and the rapid recovery of data and infrastructure in adverse situations, such as hardware failures or cyberattacks. The challenge lies in developing efficient strategies that minimize losses and enable the resumption of activities. Key elements include risk identification, contingency planning, the implementation of technological solutions, and continuous testing. The proper allocation of resources is crucial for the success of these strategies. This study proposes a procedure for disaster recovery, focusing on the protection of corporate data, which will be tested in a supermarket chain, aiming to ensure the protection of vital assets.

Keywords: Disaster Recovery; Information Technology, Infrastructure.

[1]Curso de Ciência da Computação, Universidade do Extremo Sul Catarinense (Unesc), Criciúma - Santa Catarina - Brasil. mateus_silvano@hotmail.com

[2]Orientador, Curso de Ciência da Computação, Universidade do Extremo Sul Catarinense (Unesc), Criciúma - Santa Catarina - Brasil. gustavo@unesc.net

1 INTRODUÇÃO

O problema relacionado ao Disaster Recovery (Recuperação de Desastres) em sistemas de Tecnologia da Informação (TI) consiste na necessidade de garantir a continuidade operacional e a recuperação rápida de dados, aplicativos e infraestrutura de TI em caso de eventos catastróficos, como falhas de hardware, ataques cibernéticos, desastres naturais ou qualquer outra situação que interrompa as operações normais de uma organização. Esses eventos podem resultar em perda de dados, tempo de inatividade prolongado, danos à reputação da empresa e impactos financeiros significativos (Moras; Terence; Filho, 2004).

Portanto, o desafio reside em desenvolver e implementar estratégias eficazes de recuperação de desastres que minimizem os danos e permitam à organização retomar suas operações normais o mais rapidamente possível.

Conforme Jesus (2018) os principais aspectos do problema incluem a identificação de riscos, o planejamento de contingência a implementação de soluções tecnológicas e os testes de atualização contínuos. Dentro desse contexto, cabe ressaltar que a alocação de recursos adequados, incluindo pessoal, orçamento e tecnologia é fundamental para garantir a implementação bem-sucedida e a manutenção contínua das estratégias de recuperação de desastres.

Em resumo, o problema de recuperação de desastres em sistemas de TI envolve a necessidade de proteger os ativos críticos de uma organização e garantir sua disponibilidade contínua, mesmo diante de eventos adversos imprevistos.

Diante disso, o presente trabalho tem como objetivo o desenvolvimento de um modelo de processo que aborda a Recuperação de Desastres (DR) aplicado na segurança de dados empresariais para garantir a continuidade operacional e a proteção dos dados críticos da empresa diante de eventos adversos que possam interromper suas operações normais.

A metodologia proposta, é pautada nas melhores práticas para modelagem e execução do processo o qual deverá ser apresentando através de um conjunto de atividades e tarefas encadeadas bem como a sua validação deverá ser executada em uma empresa do segmento de supermercados com operação crítica.

2 DISASTER RECOVERY

O DR ou Disaster Recovery é um processo de recuperação de ambiente de TI de uma empresa após um incidente. Ao usá-lo, é possível lidar rapidamente com os vários problemas que podem afetar uma organização, como catástrofes naturais, atividades de cibercriminosos e problemas internos e assim podendo garantir a continuidade dos negócios, mitigar os efeitos de desastres, manter a integridade dos dados corporativos e mitigar os efeitos negativos (Synnex, 2023).

Segundo Wallace e Webber (2020, tradução nossa) as técnicas de DR inicialmente eram principalmente físicas, com a criação de locais alternativos e a realização de backups físicas de dados. No entanto, as abordagens ao DR se tornaram mais sofisticadas e abrangentes com o avanço das tecnologias digitais e o aumento das ameaças cibernéticas. As soluções incluem a replicação de dados em tempo real e o uso de nuvens computacionais para maior resiliência.

Este conceito é uma parte essencial do planejamento de continuidade de negócios (BCP) com foco na recuperação de sistemas de TI, porém o plano de continuidade de negócios incluem técnicas para organizar os processos empresariais (Snedaker, 2014, tradução nossa).

Conforme Fagundes (2023) a ISO 22301 define as condições para planejar, estabelecer, implementar, operar, monitorizar, rever, manter e melhorar continuamente um sistema de gestão com o objetivo de responder eficazmente a eventos que possam interromper o funcionamento normal de uma organização. O objetivo da ISO 22301 é que seja aplicável a todas as organizações, independentemente de seu tipo, tamanho ou natureza

O DRP deve conter uma documentação com instruções detalhando as etapas necessárias para reiniciar todos os serviços ou apenas os serviços críticos, permitindo a retomada das operações. O documento deve fornecer uma lista de eventos necessários para preparar o local de backup, bem como as tarefas e obrigações de todos os funcionários envolvidos (Ávila; Soldan; Neto, 2017).

2.1 IMPORTÂNCIA DO DISASTER RECOVERY

A importância do Disaster Recovery (DR) nas organizações modernas não pode ser subestimada. Em uma empresa onde cada vez mais dependente da tecnologia e da informação digital, a capacidade de recuperar rapidamente sistemas e dados após um evento catastrófico é crucial para a continuidade dos negócios. Eventos inesperados, como desastres

naturais, falhas de hardware, ataques cibernéticos e erros humanos, podem resultar em interrupções significativas nas operações, causando perdas financeiras, danos à reputação e até mesmo o encerramento de atividades (Sgorlon, 2021).

Conforme Menezes (2023) o planejamento e a implementação de um robusto plano de Disaster Recovery garantem que uma organização esteja preparada para responder a esses eventos adversos de maneira eficaz. Um DR bem estruturado envolve a criação de procedimentos detalhados para a recuperação de sistemas críticos, a replicação de dados em locais secundários seguros e a execução de testes regulares para assegurar a eficácia dos processos de recuperação. Essa preparação não apenas minimiza o tempo de inatividade, mas também assegura que os dados essenciais sejam preservados e que as operações possam ser retomadas o mais rapidamente possível.

Segundo Almeida (2021) além da proteção direta aos ativos tecnológicos e operacionais, o Disaster Recovery desempenha um papel fundamental na gestão de riscos e na conformidade regulatória. Muitas indústrias são regidas por regulamentações que exigem a implementação de medidas de DR para proteger dados sensíveis e assegurar a continuidade dos serviços. A falha em atender a esses requisitos pode resultar em penalidades legais e financeiras severas, além de prejudicar a confiança dos clientes e parceiros de negócios.

O investimento em estratégias de Disaster Recovery contribui para a resiliência organizacional. Em um mercado competitivo e dinâmico, a capacidade de uma empresa de se recuperar rapidamente de interrupções pode ser um diferencial estratégico. Empresas resilientes não apenas protegem seus próprios interesses, mas também demonstram um compromisso com a estabilidade e a segurança aos seus clientes, investidores e stakeholders. Portanto, o Disaster Recovery não é apenas uma medida de segurança, mas uma componente essencial da estratégia de continuidade e crescimento sustentável de qualquer organização (Odata, 2023).

2.2 PLANEJAMENTO

Um plano de recuperação de desastres é uma lista abrangente de coisas que devem ser feitas antes, durante e após um desastre. A documentação e o teste do plano são necessários para garantir a continuidade das operações e a disponibilidade de recursos críticos em caso de desastre (Jesus, 2018).

Os gestores de TI em ambientes corporativos devem estabelecer uma rotina eficaz e uma infraestrutura de TI robusta para otimizar os processos de recuperação de dados sem comprometer a produtividade da empresa. Assim, é necessário definir um RPO e RTO adequado para atender às necessidades da empresa (Sirtoli, 2022).

Conforme Snedaker (2014, tradução nossa) um bom planejamento é essencial para o ciclo de recuperação de desastres. Mitigação, preparação, resposta e recuperação são as quatro fases do ciclo:

a) Mitigação: Inclui procedimentos destinados a eliminar ou diminuir a vulnerabilidade aos impactos de desastres. O planejamento para mitigação inclui organizar os recursos; avaliação de riscos; criação, implementação e revisão de planos para mitigação, implementação e revisão de estratégias. O planejamento ajuda os gerentes a tomar boas decisões na fase de mitigação baseado em dados de avaliação de risco e perigos substanciais para diminuir os riscos de ameaças futuras;

b) Preparação: Refere-se às atividades e programas que fornecem informações sobre como preparar melhor uma organização e uma outra para um desastre. O treinamento podem ajudar na resposta e recuperação de desastres. A preparação para uma catástrofe requer a consideração da pior possível situação que poderia causar prejuízos à sua organização;

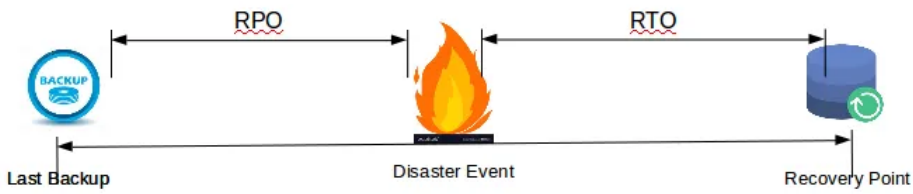
c) Resposta: Refere-se às medidas implementadas imediatamente após um desastre. A prioridade é reduzir os efeitos negativos, minimizar danos e restabelecer a funcionalidade essencial no menor período de tempo possível. Isso engloba a execução de planos de emergência, a mobilização de recursos, a comunicação eficiente entre os envolvidos e as medidas de contenção do incidente;

d) Recuperação: É o período no qual a organização se esforça para restabelecer a normalidade após um desastre. Abrange ações de curto e longo prazo, tais como consertos, retomada de operações, avaliação de prejuízos e execução de aprimoramentos fundamentados em lições apren-

didas. A meta é reconstruir de maneira resiliente e estar mais apto para eventos futuros.

Segundo Neris (2023) o Recovery Time Objective (RTO) é a duração máxima em que o sistema deve ser restaurado após uma catástrofe. Essa métrica é crucial porque o impacto sobre as operações do negócio aumenta com o tempo que um sistema fica inativo e o Recovery Point Objective (RPO) é ponto em que os dados devem ser recuperados após uma catástrofe. Isso significa que os dados devem ser recuperados até o ponto em que estavam protegidos em caso de falha ou ataque (Figura 1)

Figura 1 - RPO e RTO



Fonte: Nanayakkara (2020).

3 BACKUP

Backup é um termo inglês que pode ser traduzido como cópia de segurança (Andrade, 2023).

Segundo J. e Schimiguel (2018) o objetivo do backup é garantir que os dados sejam copiados em uma mídia secundária, caso o conteúdo original seja perdido, destruído, corrompido, infectado por vírus ou até mesmo sequestrado, esta cópia é armazenada e guardada para uso posterior.

O backup permite a restauração dos dados perdidos no caso de perda dos arquivos originais. Assim, é possível entendê-lo como um procedimento para garantir que o sistema de TI esteja seguro. Como resultado, o backup é necessário para proteger tanto o hardware quanto o software, bem como os bancos de dados e arquivos (Silva, 2022).

Conforme Moraes (2007) o backup requer um plano claro que atenda aos objetivos de cada empresa. Para isso, é necessário criar e

manter uma estratégia de backup contínua que proteja os dados pertinentes.

3.1 MODELOS DE BACKUP

Santos (2018) define em três tipos de backups principais como:

a) Backup completo: Este tipo de backup, chamado também de backup Full, realiza cópias indiscriminadas de todos os arquivos escolhidos, independentemente de terem sido alterados. Este tipo de backup requer mais espaço de armazenamento porque, independentemente de alterações nos arquivos, todos os dados (alterados ou não) serão gravados ao fazer um novo backup. Este método é normalmente usado como base para os outros métodos;

b) Backup incremental: Este método é diferente do backup completo, que copia todos os arquivos. Ele copiará apenas os arquivos que foram modificados ou adicionados desde o backup mais recente. O backup incremental tem como vantagem o melhor desempenho em sua criação em comparação com o backup completo, pois apenas serão copiados os arquivos que foram criados ou alterados após a data do backup mais recente. Para fazer um backup incremental, um backup completo é usado primeiro e os restantes são feitos de forma incremental. Este tipo de backup requer menos espaço de armazenamento em mídia do que backups completos, pois serão gravados apenas arquivos específicos e não a totalidade dos arquivos;

c) Backup diferencial: Se assemelha ao incremental, pois só copiará arquivos novos e alterados após o backup completo mais recente. No entanto, os procedimentos utilizados no tipo diferencial são cumulativos, o que significa que quando um arquivo é alterado ou criado, ele será inserido em todos os backups diferenciais subsequentes. Se usar o tipo de backup diferencial, como apenas serão copiados os arquivos que foram criados ou alterados após a data do último backup completo, terá um melhor desempenho e menos espaço de armazenamento. No entanto, ao criar um novo

conjunto de backups, o tamanho do backup aumentará gradualmente como resultado da acumulação.

4 CONTINUOUS DATA PROTECTION

Conforme Safety (2023) a Proteção Contínua de Dados (CDP) é um método de backup incremental que registra ou monitora continuamente as alterações nos dados. O monitoramento contínuo possibilita ao CDP identificar as mudanças nos dados em tempo real, à medida que são realizadas. Assim, as informações se tornam acessíveis imediatamente após serem criadas ou modificadas.

Esta técnica, de forma inteligente diminui o volume de dados que devem ser copiados em cada ciclo de backup, eliminando a incômoda "janela"de tempo. Sob essa ótica, as cópias de segurança são feitas a cada poucos minutos, e não apenas uma vez por noite (Julio, 2020).

5 METODOLOGIA

Para a criação deste projeto, foi conduzido um estudo bibliográfico sobre os conceitos de disaster recovery. Foi necessário projetar e construir máquinas virtuais para simular um ambiente similar a um ambiente supermercadista, a fim de realizar os experimentos requeridos.

Foi desenvolvido um Plano de Recuperação de Desastres para o ambiente supermercadista onde os testes foram realizados com o objetivo de garantir a segurança das informações. Foram elaboradas três tabelas que detalham os cenários de desastre, as responsabilidades dos técnicos e os prazos previstos para a retomada das atividades e uma tabela que define os parâmetros RTO e RPO. Os testes foram realizados simulando eventos que poderiam comprometer a integridade dos dados e a operação dos sistemas.

6 TESTES

Para a execução dos testes, adotou-se o plano passo a passo com a utilização do software Veeam Backup & Replication simulando o surgimento de um evento para cada uma das três tabelas de desastres criadas no DR. Estes testes visam confirmar se o DR criado está realmente proporcionando a segurança esperada para os dados do ambiente.

6.1 TABELAS DE CENÁRIOS DE DESASTRE

As tabelas a seguir descrevem os cenários de desastre identificados, estimando o prazo para reestabelecimento do desastre. O prazo foi determinado juntamente com o gerente da área onde foi executado os testes.

Tabela 1 – Desastre por Atualização de Software

Definição do Desastre	Atualizações malsucedidas dos sistemas
Responsável Técnico	TI da empresa
Prazo Estimado para Reestabelecimento	3 horas

Fonte: Do Autor.

Tabela 2 – Desastre por Perda de Dados

Definição do Desastre	Falhas com ou sem interação humana que ocasionem perda ou modificação de dados
Responsável Técnico	TI da empresa
Prazo Estimado para Reestabelecimento	30 minutos

Fonte: Do Autor.

Tabela 3 – Desastre por Defeito em Hardware

Definição do Desastre	Falhas com ou sem interação humana que ocasionem defeitos de hardware
Responsável Técnico	TI da empresa
Prazo Estimado para Reestabelecimento	30 minutos

Fonte: Do Autor.

Tabela 4 – RTO e RPO dos Sistemas

	RTO	RPO
Sistema ERP	30 minutos	1 minuto
Sistema Spaceman	3 horas	1 hora

Fonte: Do Autor.

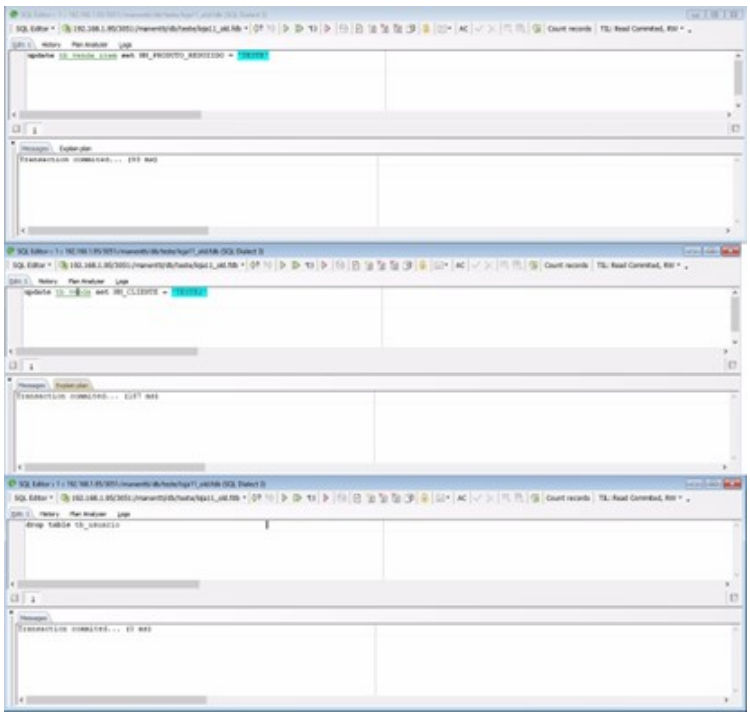
6.2 TESTES REALIZADOS

Os testes foram conduzidos para avaliar a eficácia do DR em cenários simulados:

6.2.1 Teste 1

No primeiro teste foi simulada uma falha que deixou todos os dados iguais por uma falha humana. Para realizar o teste o banco de dados do sistema ERP recebeu vários comandos, conhecidos como "updates". não incluindo nenhuma cláusula do tipo "where"na tabela de venda itens. Também foi executado o comando do tipo "drop table"foi executado na tabela de usuários (Figura 2).

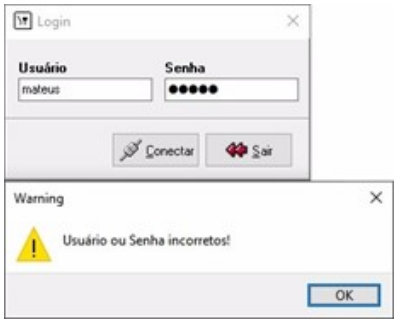
Figura 2 - Updates



Fonte: Do Autor.

Com todas essas modificações realizadas por erro humano, bem como uma variedade de dados terem perdido sua autenticidade e, como a tabela de usuários não existia mais, não foi mais possível acessar o sistema (Figura 3).

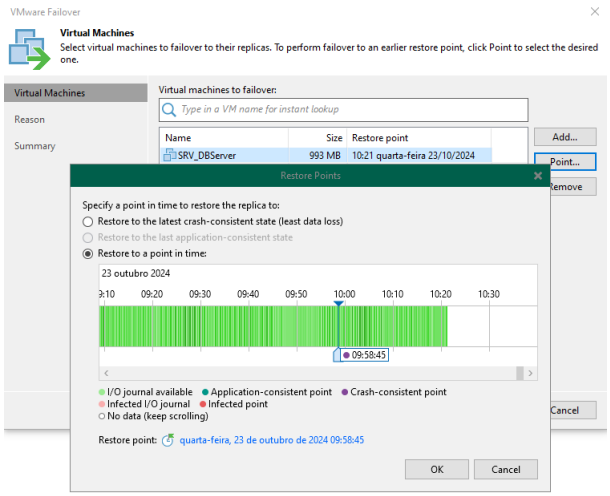
Figura 3 - Erro após Updates



Fonte: Do Autor.

Para a correção do problema, foi consultado o ultimo Point CDP da VM do Banco de Dados que estava armazenado em outro servidor. (Figura 4).

Figura 4 - CDP Point Banco de Dados



Fonte: Do Autor.

Após a restauração a aplicação voltou a funcionar normalmente (Figura 5).

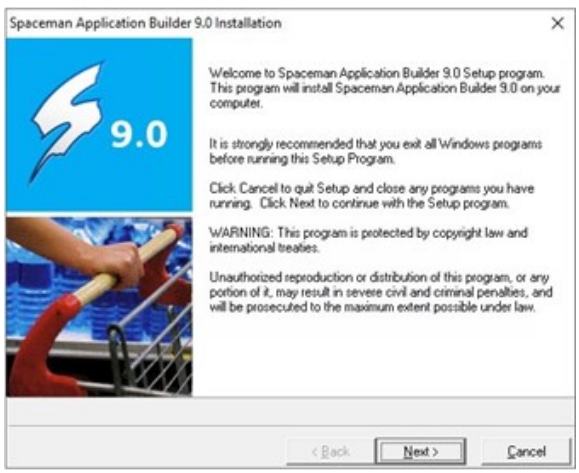
Figura 5 - Acesso ERP

Fonte: Do Autor.

6.2.2 Teste 2

O teste simulou uma atualização de software malsucedida no sistema de planogramas do cliente, que no cenário criado está instalado com sua versão 11. Para tentar causar o problema foi feito download do Spaceman versão 9, e foi substituído a pasta C:\Program Files (x86) \Nielsen\Spaceman da versão instalada pela pasta de mesmo nome da antiga versão, pasta essa que possui arquivos de configuração (Figura 6).

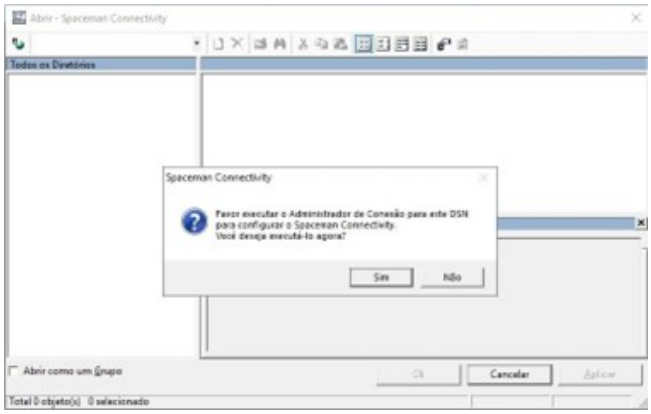
Figura 6 - Atualização Software



Fonte: Do Autor.

Com isso não foi mais possível acessar o sistema (Figura 7).

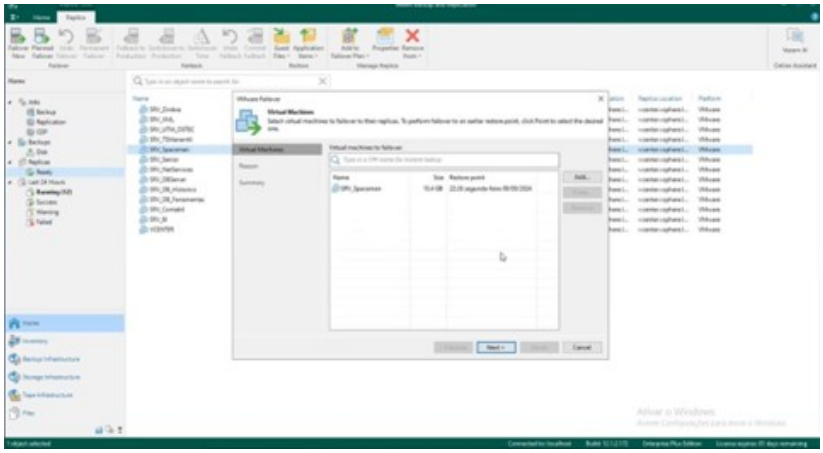
Figura 7 - Erro acesso Software



Fonte: Do Autor.

Para a correção do problema, foi consultado o ultimo CDP da VM realizado do sistema Spaceman que estava armazenado em outro servidor. (Figura 8).

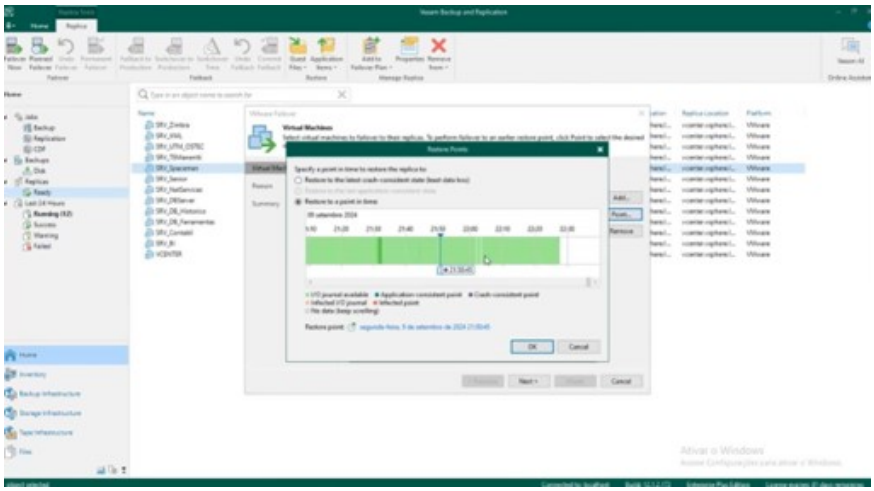
Figura 8 - CDP Veeam



Fonte: Do Autor.

Verificado o point time que deseja restaurar (Figura 9).

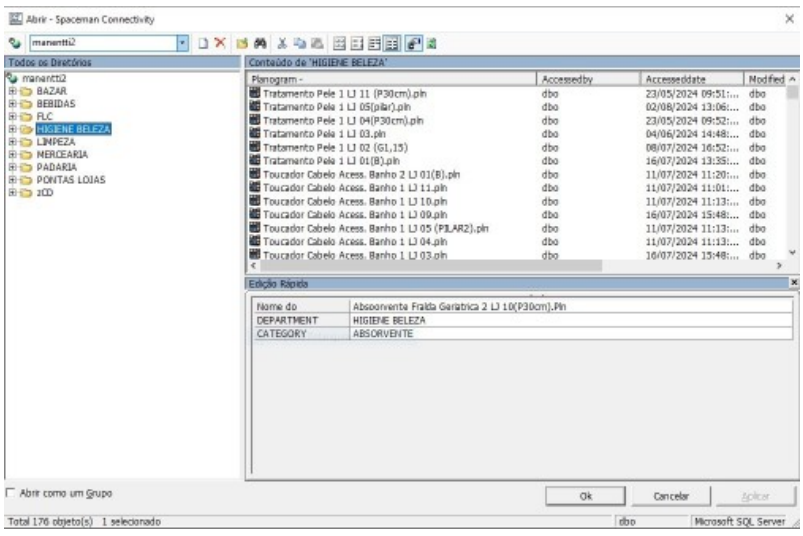
Figura 9 - Point Time CDP



Fonte: Do Autor.

Após a restauração a aplicação voltou a funcionar normalmente (Figura 10).

Figura 10 - Spaceman



Fonte: Do Autor.

6.2.3 Teste 3

O teste seguinte simulou uma falha causada por problemas no hardware. desta vez, um erro que não foi resultado de intervenção humana. Simulou-se que o problema afetou a memória do servidor, que nesse cenário o servidor se desligou de maneira inesperada. Realizado a substituição ou remoção da memória que estaria danificada, depois da substituição ou remoção o equipamento foi ligado e foi analisado para determinar se algum sistema foi impactado com esse desligamento.

7 RESULTADOS E DISCUSSÕES

Como resultado deste estudo foi desenvolvido e testado um Disaster Recovery para um ambiente empresarial do setor de supermercados com funcionamento crítico. Com o ambiente adequadamente preparado, um DR foi estabelecido com o objetivo de seguir as melhores práticas de recuperação.

O plano incluiu as especificações identificadas na pesquisa bibliográfica, incluindo diretrizes para a realização de cópias de segurança de cada sistema e dados do ambiente, prazo estimado para recuperação e medidas a serem implementadas pelos participantes após a ocorrência de cada tipo de desastre mencionado.

A etapa de testes incluiu simulações de catástrofes no cenário com o objetivo de serem o mais parecidos possível com uma situação real. Foram realizados três experimentos com diversos tipos de desastres e em todas as simulações de desastres a recuperação dos sistemas e dados ocorreu com sucesso, em um intervalo de tempo inferior a que estava programado para retomar as atividades, realizando com êxito o RTO e RPO definidos para cada sistema corporativo.

Com o objetivo de alcançar esses resultados positivos e melhorar o modelo de backup, foi criado um cenário onde os backups e replicas seriam executados de maneira automatizada. Para realizar os backup e replica, optou-se por utilizar um programa chamado Veeam Backup & Replication, que permite a programação de tarefas para backup e CDP de forma automatizada.

O resultado da automação foi extremamente gratificante, pois atingiu o objetivo proposto, que era fazer cópias de segurança de todos os sistemas e dados, além de realizar a limpeza dos dados antigos, sem a necessidade de intervenção humana direta.

8 CONCLUSÃO

Essa pesquisa teve o objetivo a implementação de um processo de Recuperação de Desastres (DR) voltado para a proteção de dados corporativos se revelou crucial para assegurar a continuidade das operações diante de eventos desfavoráveis. O estudo revelou que, ao implementar as melhores práticas na modelagem e implementação deste processo, as organizações podem não só salvaguardar seus dados vitais, mas também reduzir riscos consideráveis ligados a interrupções nas operações.

A metodologia sugerida, foi aplicada em uma companhia do setor de supermercados, que opera em um cenário crítico e extremamente volátil. Esta validação não apenas confirmou a efetividade do modelo, mas também destacou a relevância de adaptar as estratégias de recuperação às necessidades particulares de cada entidade.

Em resumo, a criação de um processo de recuperação de desastres sólido e claramente estabelecido é uma estratégia crucial para qualquer organização que deseja resiliência e segurança em suas atividades. As conclusões desta pesquisa podem ser utilizadas como fundamento para pesquisas futuras e para a aplicação prática em várias indústrias, auxiliando assim na construção de um ambiente de negócios mais seguro e sustentável.

REFERÊNCIAS

ALMEIDA, A. **Disaster Recovery: como criar um plano de recuperação de desastres**. 2021. Acesso em: 16 jun. 2024. Disponível em: <https://blog.hosts.green/disaster-recovery/>.

ANDRADE, L. S. de. **Política de backup e restauração: um estudo de caso em uma cooperativa de trabalho médico**. 2023. Acesso em: 24 abr. 2024. Disponível em: <https://www.monografias.ufop.br/bitstream/35400000/6073/6/MONOGRAFIA_Pol%c3%adticaBackupRestaura%c3%a7%c3%a3o.pdf>.

FAGUNDES, E. **Disaster Recovery Plan (DRP)**. 2023. Acesso em: 26 mai. 2024. Disponível em: <https://efagundes.com/artigos/disaster-recovery-plan-drp/>.

J., G. B. A.; SCHIMIGUEL, G. **IMPLEMENTAÇÃO DE BACKUP COMO PROCESSO DE SEGURANÇA DA INFORMAÇÃO**. 2018. Acesso em: 23 abr. 2024. Disponível em: <http://www.eumed.net/2/rev/atlante/2018/02/backup-seguranca-informacao.html>.

JESUS, R. C. de. **PLANEJAMENTO DA RECUPERAÇÃO DE DESASTRES PARA EMPRESAS COM BAIXA VOLUMETRIA DE**

DADOS. 2018. Acesso em: 03 mai. 2024. Disponível em: <https://spo.ifsp.edu.br/images/phocadownload/DOCUMENTOS_MENU_LATERAL_FIXO/POS_GRADUA%C3%87%C3%83O/ESPECIALIZA%C3%87%C3%83O/Gest%C3%A3o_da_Tecnologia_da_Informa%C3%A7%C3%A3o_____/PRODUCAO/2018/Planejamento_da_Recupera%C3%A7%C3%A3o_de_Desastres_para_Empresas_com_Baixa_Volumetria_de_Dados.pdf>.

JULIO, C. **Continuous Data Protection (CDP): entenda o conceito e suas vantagens para as empresas**. 2020. Acesso em: 23 out. 2024. Disponível em: <https://backupgarantido.com.br/blog/continuous-data-protection/>.

MENEZES, V. **Supere os desafios de implementação de um plano de disaster recovery**. 2023. Acesso em: 16 jun. 2024. Disponível em: <https://blog.equinix.com/blog/2023/08/15/supere-os-desafios-de-implementacao-de-um-plano-de-disaster-recovery/>.

MORAES, E. M. **PLANEJAMENTO DE BACKUP DE DADOS**. 2007. Acesso em: 23 abr. 2024. Disponível em: <http://repositorio.unitau.br/jspui/handle/20.500.11874/6001>.

MORAS, G. D. d. A.; TERENCE, A. C. F.; FILHO, E. E. A TECNOLOGIA DA INFORMAÇÃO COMO SUPORTE À GESTÃO ESTRATÉGICA DA INFORMAÇÃO NA PEQUENA EMPRESA. **Revista de Gestão da Tecnologia e Sistemas de Informação**, p. 27–43. ISSN 18071775. Disponível em: <https://www.scielo.br/j/jistm/a/xqSpx59SPsNH7PFTDs6JvJc/?format=pdf&lang=pt>.

NANAYAKKARA, C. **AWS Disaster Recovery Scenarios**. 2020. Acesso em: 25 abr. 2024. Disponível em: <https://crishantha.medium.com/aws-disaster-recovery-scenarios-1e8234109e79>.

NERIS, A. **O que é RPO e RTO? Conheça essas métricas de política de backup**. 2023. Acesso em: 14 mai. 2024. Disponível em: <https://amti.com.br/blog/rpo-e-rto/>.

ODATA. **Protegendo seu Data Center: melhores práticas para criar um plano de recuperação de desastres**. 2023. Acesso em: 16 jun. 2024. Disponível em: <https://odatacolocation.com/blog/plano-de-recuperacao-de-desastres/>.

SAFETY. **Continuous Data Protection: O Que É E Quais As Vantagens**. 2023. Acesso em: 23 out. 2024. Disponível em: <https://www.safetybackup.com.br/post/continuous-data-protection-o-que-e-e-quais-as-vantagens/9/>.

SANTOS, B. B. A. dos. **BACKUP CORPORATIVO COM ALTA RETENÇÃO: SUBSÍDIOS PARA CONSTRUÇÃO DA ARQUITETURA**. 2018. Acesso em: 24 abr. 2024. Disponível em: <https://bdtd.ucb.br:8443/jspui/bitstream/tede/2616/2/BrunoBelarminioAparecidodosSantosDissertacao2018.pdf>.

SGORLON, A. **O que é Disaster Recovery? Saiba tudo sobre o processo**. 2021. Acesso em: 16 jun. 2024. Disponível em: <https://sga.com.br/o-que-e-disaster-recovery/>.

SILVA, A. F. M. da. **SISTEMAS DE BACKUP: UM COMPARATIVO ENTRE BACULA COMMUNITY E GOOGLE DRIVE PARA EMPRESAS**. 2022. Acesso em: 24 abr. 2024. Disponível em: <https://repository.ufrpe.br/bitstream/123456789/3183/1/tcc_aluiziofelipemirandadasilva.pdf>.

SIRTOLI, M. A. **ANÁLISE COMPARATIVA DE FERRAMENTAS DE BACKUP**. 2022. Acesso em: 15 mai. 2024. Disponível em: <https://repositorio.ucs.br/xmlui/bitstream/handle/11338/11537/TCC%20Marco%20Antonio%20Sirtoli.pdf?sequence=1&isAllowed=y>.

SNEDAKER, S. **Business Continuity and Disaster Recovery Planning for IT Professionals**. [S.l.]: Syngress Publishing, Inc, 2014. ISBN 9781597491723.

SYNNEX, T. **DISASTER RECOVERY: O QUE É E POR QUE É FUNDAMENTAL PARA A CONTINUIDADE DOS NEGÓCIOS?** 2023. Acesso em: 15 mai. 2024. Disponível em: <https://blog-pt.lac.tdsynnex.com/disaster-recovery-o-que-e-por-que-e-fundamental-para-a-continuidade-dos-negocios

WALLACE, M.; WEBBER, L. **The disaster recovery handbook: a stepbystep plan to ensure business continuity and protect vital operations, facilities, and assets**. 2020. Acesso em: 26 mai. 2024. Disponível em: <https://www.yourhomeworksolutions.com/wp-content/uploads/edd/2020/09/the_disaster_recovery_handbook_1.pdf/>.

ÁVILA, C. S. d.; SOLDAN, E. L.; NETO, S. P. **A SEGURANÇA DE UMA ESTRUTURA DE DISASTER RECOVERY PLAN EM CLOUD COMPUTING**. 2017. Acesso em: 15 mai. 2024. Disponível em: <https://ensaios.usf.edu.br/ensaios/article/view/61>.