ESTRATÉGIA DE RESILIÊNCIA CIBERNÉTICA: UM ESTUDO DE CASO DE PLANO DE RECUPERAÇÃO DE DESASTRES (DRP) PARA INFRAESTRUTURA DE TI EM OPERAÇÕES LOGÍSTICAS

MARCUS VINICIUS DAMASCENO PEREIRA[1]
CLAYTON EDUARDO DOS SANTOS[2]

RESUMO

Este artigo apresenta um modelo prático de Plano de Recuperação de Desastres (DRP) para ambientes de Tecnologia da Informação (TI), fundamentado nas diretrizes do NIST SP 800-34 e SP 800-160 Vol. 2 e validado por meio de um estudo de caso focado em operações logísticas. A pesquisa analisa a continuidade de negócios e a recuperação segura através de um estudo de caso aplicado à MVDP Tech. O estudo avalia a recuperação de dispositivos de borda (edge devices), incorporando métricas como RTO, RPO e MTTR. Os resultados revelam que a integração entre automação de provisionamento, microsegmentação de rede e validação de integridade reduziu o MTTR médio em 64,1% em relação aos processos manuais tradicionais, validando a eficácia da arquitetura para mitigar riscos de reinfecção, reduzir a variabilidade operacional e aumentar a previsibilidade técnica em cenários de desastre.

Palavras-chave: Plano de Recuperação de Desastres. NIST SP 800-34. *CIS Controls v8*. Continuidade de negócios. Computação de borda. MTTR. *Golden Images*.

[1]E-mail: marcus.damasceno@aluno.ifsp.edu.br
[2]Coautor / Orientador. Professor Orientador no Instituto Federal de Educação, Ciência e Tecnologia de São Paulo – Campus Bragança Paulista. E-mail: claytones@ifsp.edu.br

CYBER RESILIENCE STRATEGY: A DISASTER RECOVERY PLAN (DRP) CASE STUDY FOR IT INFRASTRUCTURE IN LOGISTICS OPERATIONS

ABSTRACT

This paper presents a practical Disaster Recovery Plan (DRP) model for Information Technology (IT) environments, grounded in NIST SP 800-34 and NIST SP 800-160 Vol. 2 guidelines and validated through a case study focused on logistics operations. The research analyzes business continuity and secure recovery through a case study applied to MVDP Tech. Through controlled simulations involving 30 critical edge devices, the study evaluates the recovery of edge devices, incorporating key metrics such as RTO, RPO, and MTTR. The results demonstrate that integrating provisioning automation, network micro segmentation, and integrity validation reduced the average MTTR by 64.1% compared to traditional manual processes. These findings validate the framework's effectiveness in mitigating reinfection risks, reducing operational variability, and increasing technical predictability during disaster scenarios.

Keywords: *Disaster Recovery Plan. NIST SP 800-34. CIS Controls v8. Business Continuity. Edge Computing. MTTR. Golden Images.*

1. INTRODUÇÃO

A crescente dependência de sistemas digitais e a sofisticação das ameaças cibernéticas, como o ransomware, tornaram a infraestrutura de TI o sistema nervoso central das operações modernas. Para empresas como a MVDP Tech, que operam na interseção entre tecnologia e logística, qualquer interrupção digital reflete imediatamente em paralisia física e prejuízos financeiros.

Além do impacto operacional imediato, incidentes cibernéticos em ambientes corporativos modernos tendem a provocar efeitos em cascata: indisponibilidade de sistemas de apoio, paradas em processos críticos, perda de rastreabilidade e aumento do retrabalho. Em organizações com operação contínua e forte dependência de dispositivos finais: coletores, terminais móveis, estações de trabalho e periféricos de produção, a capacidade de restaurar rapidamente o "estado confiável" do parque tecnológico passa a ser tão relevante quanto a restauração de servidores e serviços centrais. Para evidenciar a criticidade dessa rápida recomposição, torna-se necessário mapear como a indisponibilidade desses ativos locais propaga-se de forma sistêmica e imediata por toda a cadeia de execução logística, conforme ilustrado na Figura 1:



Figura 1 – Efeitos em cascata e impactos operacionais de um ataque de ransomware na infraestrutura local. Fonte: Elaborado pelo autor (2026).

Assim, o Plano de Recuperação de Desastres (DRP - Disaster Recovery Plan) precisa contemplar não apenas a recuperação de dados, mas também a recomposição segura do ambiente, reduzindo o risco de reinfecção e garantindo integridade pós-recuperação.

A MVDP Tech atua no comércio e distribuição de hardware de alto desempenho, como GPUs (Graphics Processing Units / Unidades de Processamento Gráfico), CPUs (Central Processing Units / Unidades Centrais de Processamento) e memórias, com operação logística intensiva baseada em Centros de Distribuição (CDs) . Nesses ambientes, dispositivos finais (end devices), como notebooks de packing, coletores Android (handhelds) e impressoras térmicas, são essenciais para a execução de processos críticos, incluindo recebimento, separação (picking), expedição e rastreabilidade de pedidos.

A indisponibilidade desses ativos compromete diretamente o fluxo logístico, causando represamento de cargas, aumento de retrabalho e risco de descumprimento de SLAs (Service Level Agreements / Acordos de Nível de Serviço) de entrega. Assim, o DRP precisa contemplar não apenas a continuidade de sistemas centrais, mas também a recomposição rápida e segura do parque de endpoints que sustenta a operação no "chão" do Centro de Distribuição.

Nesse contexto, a abordagem de resiliência cibernética aplicada ao DRP agrega valor ao incorporar padronização, automação e validação técnica, como o uso de imagens corporativas, isolamento de rede durante restauração e verificações de integridade. Com isso, o plano deixa de ser somente documental e passa a ser operacionalizável, mensurável e testável, aproximando a recuperação do nível de maturidade exigido por ambientes críticos. Também se torna possível alinhar o plano a indicadores de desempenho, como RTO, RPO e MTTR, favorecendo governança, auditoria e melhoria contínua do processo.

Com a realização deste trabalho, pretende-se disponibilizar ao leitor um modelo prático, replicável e empiricamente testado de resiliência cibernética aplicado à infraestrutura local de TI e computadores de trabalho. Mais do que uma revisão teórica das normas, este estudo entrega as matrizes operacionais de contingência, os fluxos detalhados de automação de imagens (Golden Images) e os resultados quantitativos

de redução de tempo de parada (MTTR) medidos na operação da MVDP Tech. O objetivo é fornecer um guia de referência que apoie tanto a tomada de decisão estratégica de gestores e engenheiros de TI, quanto a execução técnica por analistas de infraestrutura e segurança da informação.

Além disso, ao fundamentar a arquitetura em metodologias acessíveis e ferramentas reprodutíveis (como automações em Bash e utilitários de implantação), este modelo estende sua utilidade prática a pequenas e médias empresas que necessitam mitigar ataques de ransomware e aumentar sua resiliência operacional sem a exigência de investimentos proibitivos em softwares proprietários.

1.1 MOTIVAÇÃO E JUSTIFICATIVA

A necessidade deste estudo justifica-se pela interdependência crítica entre hardware e software na MVDP Tech. No cenário logístico, a falha de um único dispositivo de captura ou processamento pode interromper o fluxo de expedição, causando ociosidade de equipe e atrasos contratuais. A motivação reside na criação de uma arquitetura que garanta que o hardware retorne ao estado operacional seguro no menor tempo possível.

Em vez de apresentar valores nominais, o impacto econômico de um desastre pode ser estimado a partir de indicadores como custo de ociosidade logística e penalidades por descumprimento de SLA (Service Level Agreement) de entrega. Na MVDP Tech, a indisponibilidade dos endpoints impacta diretamente a execução das atividades operacionais e o faturamento, gerando perdas crescentes à medida que o tempo de interrupção ultrapassa o RTO estabelecido. Assim, o investimento em resiliência se justifica pela redução do risco de paralisação prolongada, pela proteção da margem operacional e pela preservação da reputação da empresa perante clientes e parceiros da cadeia de suprimentos.

Parte-se da hipótese de que a integração entre automação de provisionamento, micro segmentação e validação contínua de integridade reduz significativamente o MTTR e aumenta a previsibilidade operacional em cenários de desastre, permitindo

que a recuperação de ativos de borda ocorra dentro dos limites críticos de RTO estabelecidos pelo negócio.

1.2 DEFINIÇÕES DE RTO, RPO E MTTR NO CONTEXTO LOGÍSTICO

Para que o DRP seja mensurável, utilizam-se métricas baseadas no NIST (National Institute of Standards and Technology) SP 800-34 (NIST, 2010).

RTO (Recovery Time Objective): na MVDP Tech, estabeleceu-se um RTO limite (threshold) de 30 minutos para a operação como um todo, visando evitar o represamento crítico de cargas. Para garantir que este limite não seja ultrapassado, as metas operacionais por categoria de ativo são definidas com margens mais restritas, entre 15 e 25 minutos, conforme detalhado na Matriz de Resiliência no item 6.2.

RPO (Recovery Point Objective): representa a tolerância à perda de dados. No contexto logístico da MVDP Tech, busca-se manter valores próximos de zero para preservar a rastreabilidade dos pedidos, registros de movimentação, expedição e controle operacional.

MTTR (Mean Time to Repair/Recover): representa o tempo médio efetivamente necessário para reparar, restaurar ou recompor um ativo comprometido até seu retorno ao estado operacional seguro. Neste estudo, o MTTR é utilizado como indicador prático da eficiência da estratégia de recuperação proposta, permitindo comparar o processo manual tradicional com o modelo automatizado baseado em Golden Images, MDM (Mobile Device Management / Gerenciamento de Dispositivos Móveis), micro segmentação e validação de integridade.

2. METODOLOGIA

A presente pesquisa adota uma abordagem de métodos mistos, integrando a análise qualitativa de processos à mensuração quantitativa de métricas de recuperação. O estudo caracteriza-se como um estudo de caso único de natureza aplicada e objetivos descritivos. Conforme defendido por Creswell e Creswell (2021), a integração de dados qualitativos e quantitativos permite uma compreensão mais

completa do problema de pesquisa do que apenas uma das abordagens isoladamente. Complementarmente, utiliza-se a fundamentação de Yin (2015) para estruturar o estudo de caso como estratégia ideal para investigar fenômenos contemporâneos em seus contextos reais, o que se aplica à análise da resiliência cibernética na MVDP Tech.

O desenho metodológico foi estruturado em quatro fases sistemáticas:

Levantamento e Diagnóstico Normativo: realizou-se uma pesquisa documental baseada nas diretrizes NIST SP 800-34, SP 800-53, SP 800-61 e SP 800-160 Vol. 2, alinhadas aos controles de defesa ativa do CIS Critical Security Controls Version 8 . Esta fase visou estabelecer os requisitos de resiliência e conformidade necessários para suportar operações de alta disponibilidade no setor logístico.

Desenvolvimento do Artefato de Recuperação: consistiu na construção técnica de um pipeline de automação e na criação de Golden Images, ou imagens padronizadas. O objetivo foi garantir a imutabilidade do ambiente restaurado e a aplicação ágil de configurações de segurança e rede.

Execução Experimental e Simulação de Estresse: condução de testes controlados em ambiente de laboratório com a replicação fiel do parque tecnológico da organização. Simulou-se um incidente de ransomware em 30 ativos críticos, como coletores de dados, notebooks e impressoras térmicas, utilizando a técnica de observação direta para a coleta de métricas de RTO e MTTR. Para endpoints computacionais, como notebooks e coletores de dados, a recuperação foi baseada na aplicação de imagens padronizadas, automação de configuração e validação de conformidade. Para periféricos, como impressoras térmicas, o processo concentrou-se na restauração de drivers, filas de impressão, parâmetros de rede, firmware quando aplicável e reintegração ao fluxo operacional de etiquetagem.

Validação e Análise de Integridade: os dados coletados foram confrontados com os SLAs de negócio. A integridade dos artefatos restaurados foi validada por meio de hashes SHA-256, permitindo comparar imagens, arquivos críticos e pacotes de configuração com versões previamente homologadas. Esta validação contribui para identificar alterações não autorizadas nos componentes verificados. No entanto, a ausência de persistência maliciosa deve ser confirmada por controles

complementares, como varredura por EDR (Endpoint Detection and Response / Detecção e Resposta de Endpoint)/antimalware, análise de serviços ativos, tarefas agendadas, registros de inicialização, logs de segurança e validação de conformidade antes da reintegração do dispositivo à rede produtiva.

As simulações foram restritas a um ambiente de laboratório isolado (sandbox), a fim de preservar a integridade da operação real. Embora o cenário replique as variáveis técnicas da organização, os resultados obtidos refletem o desempenho da infraestrutura e da equipe sob condições de teste e podem sofrer variações em cenários de desastres de larga escala ou interrupções totais de serviços de conectividade externa.

2.1 TRABALHOS RELACIONADOS E ANÁLISE COMPARATIVA

A evolução das estratégias de continuidade de negócios tem migrado de modelos estáticos para estruturas de resiliência cibernética proativa. No contexto de segurança de software, Alhazmi e Malaiya (2008) contribuem com modelos quantitativos para compreender o processo de descoberta de vulnerabilidades, reforçando a importância de reduzir a exposição técnica dos sistemas por meio de atualização, padronização e controle de configuração.

No âmbito da cadeia de suprimentos, Lohmer, Bugert e Lasch (2020) exploram como a resiliência é fortalecida pela digitalização e pela coordenação entre agentes, destacando que falhas em cadeias logísticas podem gerar um Ripple Effect, ou efeito cascata, comprometendo a integridade de toda a rede operacional.

A transição para modelos de Confiança Zero (Zero Trust) também redefine o DRP. Conforme as diretrizes do NIST SP 800-160 Vol. 2 (NIST, 2021), a engenharia de sistemas resilientes deve pressupor que o ambiente permanece hostil após um incidente, o que exige a validação rigorosa da integridade dos ativos antes de sua reintegração à rede. Esta visão estabelece a necessidade de mecanismos de reconstituição e restauração de componentes para um estado confiável, no qual a resiliência é maximizada por meio da recomposição rápida e automatizada dos ativos afetados. A Tabela 1 sintetiza as lacunas identificadas.

Tabela 1 – Trabalhos relacionados e lacunas identificadas

Autores / Ano	Contexto Tecnológico	Método / Abordagem	Limitação Identificada
Alhazmi e Malaiya (2008)	Vulnerability Discovery	Modelagem quantitativa	Foco em software; baixa ênfase em hardware logístico.
Lohmer et al. (2020)	Supply Chain Resilience	Simulação baseada em agentes	Abordagem voltada à cadeia de suprimentos, sem detalhamento técnico de recuperação de endpoints.
NIST SP 800-160 Vol. 2 (2021)	Cyber Resilient Systems	Framework normativo	Abordagem teórica de alto nível; carece de guias específicos para implementação em endpoints logísticos.
Proposta deste artigo	**Resilient Edge Recovery**	**Arquitetura integrada**	**Integração entre automação, micro segmentação e integridade.**

Fonte: Elaborado pelo autor (2026).

3. REFERENCIAL TEÓRICO

A evolução das ameaças cibernéticas exige que o Plano de Recuperação de Desastres (DRP) transcenda a visão tradicional de continuidade e se integre ao conceito de resiliência cibernética. Segundo Fernandes e Abreu (2014), a governança de TI em ambientes de alta criticidade deve estabelecer um alinhamento rigoroso entre os processos de recuperação e os objetivos de negócio, garantindo que o DRP atue como um framework operacional dinâmico e testável, em vez de um documento estático.

Nesse contexto, o NIST SP 800-160 Vol. 2 (NIST, 2021) define que sistemas resilientes devem possuir a capacidade de antecipar, resistir, recuperar e, fundamentalmente, adaptar-se a condições adversas. Essa visão introduz o conceito de resiliência adaptativa, sugerindo que a organização deve evoluir seu estado de segurança a partir da experiência de um incidente. Wallace e Webber (2017) corroboram essa perspectiva ao argumentar que a eficácia da recuperação está intrinsecamente ligada ao nível de automação e à redução de intervenções manuais, o que minimiza o impacto do erro humano e acelera a transição para o estado de normalidade.

No cenário brasileiro, a discussão sobre a proteção de infraestruturas críticas é reforçada por Fontes (2017), que enfatiza a segurança da informação como um processo contínuo integrado ao negócio. Para o autor, isso exige um planejamento para respostas rápidas e uma restauração controlada do parque tecnológico, visando impedir a recorrência de infecções. A literatura internacional, por meio de Sahebjamnia, Torabi e Mansouri (2015), reforça essa necessidade de sincronização, apresentando modelos de integração entre o Plano de Continuidade de Negócios (BCP) e o DRP. A resiliência organizacional, portanto, depende da capacidade de sincronizar métricas técnicas, como RTO, RPO e MTTR, com a alocação dinâmica de recursos operacionais.

Em incidentes de ransomware, a recuperação deve considerará não apenas a restauração da disponibilidade, mas também a integridade do ambiente recuperado. A simples remoção do código malicioso pode não ser suficiente quando há possibilidade de persistência, alteração de configurações ou comprometimento de componentes do sistema. Por esse motivo, a restauração a partir de uma imagem previamente homologada contribui para retornar o endpoint a um estado conhecido e confiável, desde que acompanhada por validações complementares de segurança.

Por fim, a adoção de baselines de segurança e imagens padronizadas, denominadas Golden Images, encontra sustentação no CIS Critical Security Controls Version 8 (CIS, 2021). Essa abordagem alinha-se aos controles de configuração segura preconizados pelo framework, especialmente no que se refere à manutenção de configurações padronizadas, redução da superfície de ataque, controle de ativos e garantia de integridade operacional dos endpoints corporativos. Dessa forma, após um desastre, o ambiente pode ser restaurado para um estado previamente conhecido, validado e tecnicamente confiável.

A estratégia de validação contínua e reintegração controlada adotada na MVDP Tech fundamenta-se nos princípios de Arquitetura Zero Trust (ZTA), conforme o NIST SP 800-207 (NIST, 2020b). Sob esta ótica, nenhum dispositivo é considerado confiável por padrão após um incidente, exigindo verificação rigorosa de identidade, postura de segurança e integridade antes de qualquer concessão de acesso à rede produtiva.

4. IMPACTO OPERACIONAL E ARQUITETURA DE REDE

A operação logística da MVDP Tech é caracterizada por uma alta cadência de processamento de dados em tempo real, em que a interrupção de um único nó da rede pode desencadear um efeito dominó em toda a cadeia de suprimentos. Para mitigar esse risco, a arquitetura de recuperação foi reestruturada sob os princípios de microsegmentação e privilégio mínimo, visando reduzir drasticamente o chamado Blast Radius, ou raio de explosão, de um eventual ataque. A arquitetura geral pode ser observada na Figura 2.



FIGURA 2 – Arquitetura Geral de Rede e Controle de Acesso WMS (Warehouse Management System / Sistema de Gestão de Armazém). Fonte: Elaborado pelo autor (2026).

A estratégia de resiliência baseia-se em uma topologia de rede segregada logicamente através de VLANs (Virtual Local Area Networks / Redes Locais Virtuais), orquestradas por um firewall de camada 3 (Layer 3) com inspeção profunda de pacotes (Deep Packet Inspection – DPI). Conforme as diretrizes do NIST SP 800-53

(NIST, 2020a), o controle de fluxo é garantido por Listas de Controle de Acesso (ACLs) rigorosas que impedem a movimentação lateral como detalhado na Figura 3:

a) VLAN Logística: abriga os handhelds e notebooks de packing. O tráfego é restrito aos protocolos essenciais de comunicação com o servidor WMS (Warehouse Management System / Sistema de Gestão de Armazém) .

b) VLAN de Periféricos: realiza o isolamento de impressoras térmicas e balanças industriais, ativos IoT protegidos para não servirem como vetores de ataque.

c) VLAN de Gestão: reservada para suporte técnico, com acesso via MFA (Multi-Factor Authentication / Autenticação de Múltiplos Fatores) e regras deny-by-default.

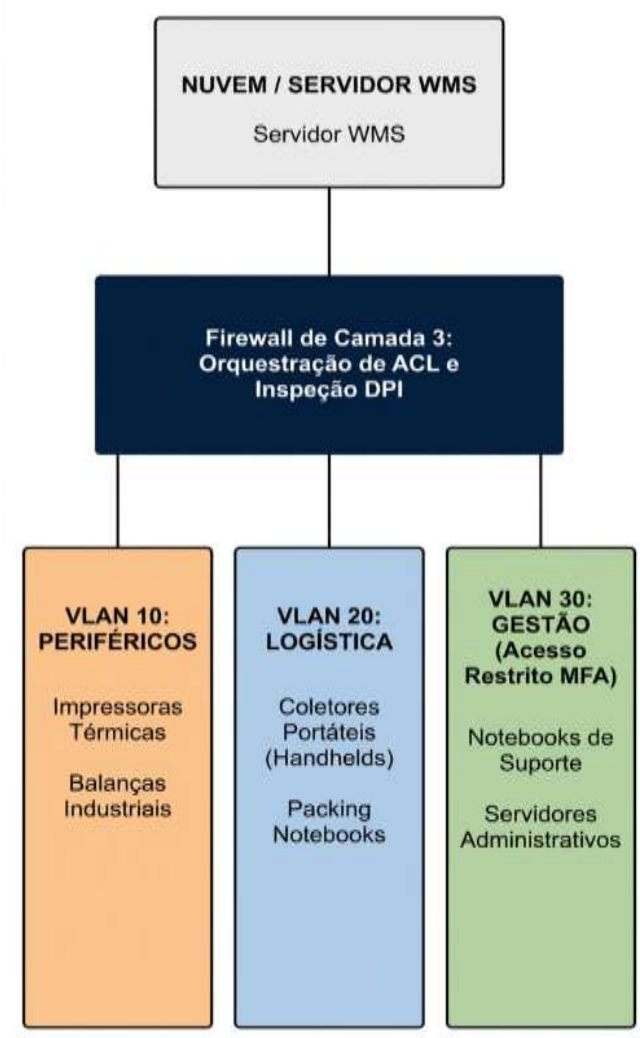


FIGURA 3 – Detalhamento da Microsegmentação e Segregação de VLANs. Fonte: Elaborado pelo autor (2026).

A comunicação com o servidor WMS em nuvem é realizada por meio de uma VPN (Virtual Private Network / Rede Privada Virtual) site-to-site, terminada no firewall de perímetro, onde são aplicadas políticas de filtragem e inspeção de tráfego. Essa arquitetura centraliza e controla o tráfego entre a rede interna e a nuvem, contribuindo para reduzir a exposição a comunicações não autorizadas originadas da internet.

Além disso, o fluxo de dados entre as VLANs internas e o ambiente em nuvem segue o princípio do privilégio mínimo, permitindo apenas as portas e destinos essenciais às transações logísticas do WMS e restringindo conexões desnecessárias, o que dificulta movimentação lateral e potenciais tentativas de exfiltração de dados.

5. ESTRATÉGIA DE RESILIÊNCIA E PADRONIZAÇÃO (GOLDEN IMAGES)

A adoção de Golden Images torna a recuperação na MVDP Tech mais previsível porque transforma a restauração em um processo padronizado, repetível e auditável. Em vez de depender de reinstalações manuais e configurações caso a caso, o que aumenta o MTTR e introduz inconsistências, a organização passa a tratar a recomposição do endpoint como uma "reentrega controlada" de um ativo pronto para produção, com sistema operacional, configurações mínimas, agentes corporativos e parâmetros de segurança previamente homologados.

Essa abordagem alinha-se aos controles de configuração segura preconizados pelo CIS Controls v8 (CIS, 2021), especialmente no que se refere à manutenção de configurações padronizadas, redução da superfície de ataque, controle de ativos e garantia de integridade operacional dos endpoints corporativos. Ressalta-se, entretanto, que Golden Images não substituem mecanismos formais de backup, mas os complementam, uma vez que sua finalidade é recompor o ambiente-base do endpoint, enquanto dados operacionais, transacionais e documentos corporativos devem permanecer protegidos por políticas específicas de backup, retenção e recuperação.

Para evitar que a padronização se torne rígida demais e inviabilize diferentes perfis de uso, recomenda-se a criação de imagens por função (role-based images). Por exemplo, pode-se separar imagens para: (a) handhelds de picking; (b) notebooks

de packing; (c) estações de suporte/gestão; e (d) terminais específicos para periféricos. Dessa forma, mantém-se uma base comum, ou baseline de segurança e conformidade, e adicionam-se apenas componentes necessários por perfil, reduzindo a superfície de ataque e facilitando a manutenção do pacote.

Como prática complementar, recomenda-se definir um controle formal de versão das imagens, por exemplo v1.0, v1.1 e v1.2, acompanhado de registro de mudanças (changelog). Cada Golden Image deve conter identificador de versão, data de criação, sistema operacional utilizado, patches aplicados, softwares incluídos, agentes de segurança instalados, responsável pela homologação, hash de integridade e status da imagem, como candidata, homologada ou obsoleta. Essa prática permite rastreabilidade, auditoria e fallback caso uma atualização introduza falhas ou incompatibilidades.

Para mitigar riscos de corrupção ou adulteração dos artefatos de recuperação, foi adotada validação de integridade por hash SHA-256. A cada versão homologada da Golden Image, bem como de seus pacotes e scripts associados, é gerado um hash de referência e registrado em repositório controlado, juntamente com o identificador de versão e o respectivo changelog. Antes da aplicação da imagem no endpoint, ou após sua transferência para a mídia offline de instalação, quando aplicável, o SHA-256 do artefato é recalculado e comparado ao valor de referência. Em caso de divergência, o procedimento de restauração é interrompido, o artefato é descartado e é acionado o fallback para uma versão estável previamente validada. A verificação por hash assegura a integridade do artefato verificado, sendo complementada por controles de acesso, governança de versões, EDR, MDM e validações de conformidade antes da reintegração à rede produtiva.

Do ponto de vista técnico, uma Golden Image robusta deve conter, no mínimo: (1) baseline do sistema operacional com atualizações críticas; (2) drivers essenciais e pacotes de compatibilidade; (3) configuração mínima de rede para permitir adesão controlada ao ambiente, como domínio ou MDM, após validação; (4) ferramentas corporativas obrigatórias, como EDR, MDM agent e inventário; e (5) políticas de hardening aplicadas no próprio build .

A estratégia também se beneficia de um modelo de restauração em fases, com separação clara entre "instalar" e "liberar acesso". A restauração utiliza uma rede de quarentena, denominada VLAN de Inspeção, na qual o tráfego é permitido exclusivamente para os endpoints de gerenciamento, como MDM e EDR. Nesta etapa, o objetivo é executar configurações e validar a conformidade. A transição da VLAN de Quarentena para a VLAN Operacional ocorre de forma dinâmica somente após o agente de segurança reportar o status de integridade e criptografia ao firewall, reduzindo o risco de um dispositivo não validado acessar o ambiente produtivo.

A manutenção das Golden Images requer rotina de atualização e governança. Recomenda-se um ciclo de revisão periódica, mensal ou bimestral, dependendo do ambiente, com janela de testes: primeiro em laboratório, depois em um grupo piloto e, por fim, distribuição para produção. Assim, a imagem se mantém alinhada a patches, mudanças de software e novos requisitos de segurança.

5.1 PIPELINE DE AUTOMAÇÃO

A operacionalização da resiliência na MVDP Tech fundamenta-se em um fluxo de trabalho estruturado e automatizado, garantindo que a recuperação não dependa de intervenções manuais propensas a erros. O pipeline de construção e armazenamento das imagens é segmentado por ecossistema tecnológico.

No ambiente Windows, a criação das Golden Images utiliza o Microsoft Deployment Toolkit (MDT), permitindo uma automação baseada em arquivos de resposta e sequências de tarefas que padronizam desde a instalação do sistema operacional até a injeção de drivers, softwares críticos e configurações corporativas. O MDT permite automatizar etapas de implantação, instalação de drivers, inclusão de aplicações e execução de scripts, contribuindo para a padronização do processo de recuperação dos endpoints (MICROSOFT, [s. d.]).

No ambiente Linux (Zorin OS), o mecanismo de geração automatizada baseia-se em ferramentas de remasterização, como o Cubic (Custom Ubuntu ISO Creator), e scripts de pós-instalação em Bash. Este processo permite a criação de uma Live

ISO customizada, que já inclui o kernel otimizado para o hardware logístico e pacotes de segurança pré-configurados.

Para mitigar gargalos logísticos em incidentes de larga escala, a MVDP Tech mantém kits de emergência pré-configurados e localizados em áreas de acesso restrito. A estratégia de distribuição não depende do envio físico de mídias pós-desastre, mas sim da existência de réplicas locais já validadas, permitindo que a restauração de múltiplos dispositivos ocorra simultaneamente sem dependência de link de dados externo.

O pipeline é regido pelos seguintes princípios técnicos adicionais: abstração de hardware, com uso de drivers universais via Sysprep; hardening, com aplicação de baselines de segurança conforme NIST SP 800-53 (NIST, 2020a); e validação criptográfica integrada ao script de inicialização da mídia offline. O instalador executa automaticamente a checagem do hash SHA-256 antes de qualquer escrita em disco. Caso ocorra divergência nos dados, o processo é abortado imediatamente com um alerta de integridade, removendo a subjetividade humana e garantindo que a imagem instalada corresponda à matriz homologada.

6. ESTUDO DE CASO E RESULTADOS

O estudo simulou a recuperação de 30 ativos críticos. O fluxo de contenção, isolamento físico e restauração automatizada adotado durante o exercício prático está detalhado na Figura 4. Para garantir a repetibilidade e a fidedignidade dos dados, os testes de recuperação foram executados em três ciclos para cada categoria de ativo, utilizando-se a média aritmética simples para a composição dos tempos finais. Cabe ressaltar que, neste estudo, o MTTR observado aproximou-se do RTO real devido ao escopo controlado da simulação, que focou no tempo técnico de restauração do "estado confiável" do hardware.



Figura 4 – Fluxo de recuperação automatizada. Fonte: Elaborado pelo autor (2026).

6.1 PROCEDIMENTOS POR CATEGORIA DE EQUIPAMENTO

Para garantir consistência operacional e reduzir o risco de reinfecção, os procedimentos de recuperação foram segmentados por categoria de ativo, respeitando dependências técnicas e testes mínimos de prontidão antes do retorno à produção.

Notebooks (Windows/Linux): iniciou-se com a limpeza completa do disco (wipe/format), visando eliminar persistências de malware. Em seguida, realizou-se o reimaging por Golden Image e a aplicação automatizada de configurações e hardening. Após a restauração, os endpoints passaram por validações de segurança,

instalação/ativação de agentes corporativos EDR/MDM e inventário e testes básicos de conectividade controlada.

Handhelds (coletores de dados): executou-se o processo de enrollment via MDM, seguido de checagens de compliance, como políticas mínimas, criptografia quando aplicável, versão do sistema e integridade do agente. Como validação funcional, foram realizados testes de leitura, scanner/código de barras e conectividade com o aplicativo de operação, como WMS.

Impressoras térmicas: por se tratar de periféricos operacionais e não de endpoints computacionais no mesmo sentido dos notebooks e coletores, o procedimento não se baseia em Golden Image completa do sistema operacional. A recuperação incluiu reset de fábrica, reconfiguração de parâmetros de rede, restauração de drivers e filas de impressão, atualização ou validação de firmware quando aplicável e testes de impressão para garantir comunicação com o fluxo operacional de etiquetagem.

6.2 MATRIZ DE RESILIÊNCIA

Tabela 2 – Matriz de resiliência por categoria de ativo

Categoria de Ativo	Função Operacional	RTO Alvo (min)	RTO Real (min)	MTTR (min)	RPO Tolerado
Handhelds	Picking (Estoque)	25	24	24	Real-time
Impressora Térmica	Etiquetagem	15	10	10	N/A
Notebook Packing	Bancada	30	27	27	< 5 min
Notebook Suporte	Apoio Local	60	27	27	15 min

Fonte: Elaborado pelo autor (2026).

6.3 ANÁLISE CRÍTICA E RESILIÊNCIA ADAPTATIVA

Os resultados obtidos na Matriz de Resiliência demonstram que a estratégia adotada estabelece uma base sólida para a resiliência adaptativa dentro da MVDP Tech. Diferente de uma abordagem de recuperação estática, a estratégia

implementada permite que o sistema evolua tecnicamente a partir do incidente, incorporando melhorias de segurança, padronização e automação ao processo de restauração.

A eficiência observada no RTO real de 24 minutos para os coletores de dados valida a eficácia da automação via MDM, eliminando gargalos históricos associados a configurações manuais. Além disso, a utilização de uma VLAN de Inspeção, ou Quarentena, atua como mecanismo de controle e feedback de segurança, garantindo que os dispositivos retornem à produção apenas após validação de conformidade.

A padronização por meio de Golden Images reduz a subjetividade humana no processo de restauração, tornando a recomposição dos endpoints mais previsível, repetível e auditável. Ao restaurar os dispositivos a partir de um estado previamente homologado, a estratégia contribui para o endurecimento imediato do parque tecnológico, mitigando configurações inseguras e vulnerabilidades que poderiam ser exploradas em ataques subsequentes. Ressalta-se, entretanto, que Golden Images não substituem mecanismos formais de backup, mas os complementam, uma vez que sua finalidade é recompor o ambiente-base do endpoint, enquanto dados operacionais e transacionais devem permanecer protegidos por políticas específicas de backup, retenção e recuperação.

6.4 ANÁLISE COMPARATIVA DE IMPACTO (BASELINE)

Tabela 3 – Comparativo entre método tradicional e modelo proposto

Ativo Crítico	Método Tradicional (Manual)	Modelo Proposto (Automação)	Ganho de Eficiência (%)
Notebook	90 min	27 min	70,0%
Coletor de Dados (Handheld)	45 min	24 min	46,6%
Impressora Térmica	35 min	10 min	71,4%
Média Geral	56,6 min	20,3 min	64,1%

Fonte: Elaborado pelo autor (2026).

A análise dos dados evidencia que a automação de provisionamento não apenas acelera o retorno operacional em 64,1% na média geral, mas também estabelece um patamar de previsibilidade técnica essencial para a continuidade de negócios. Ao substituir fluxos manuais por processos orquestrados, a arquitetura reduz a variabilidade operacional inerente às execuções manuais e contribui para maior consistência no tempo de resposta e recuperação dos ativos críticos.

7. VALIDAÇÃO DE SEGURANÇA E COMPLIANCE

Para assegurar a integridade pós-recuperação, utiliza-se proteção ativa por EDR e Compliance Check via MDM. Somente após a validação de requisitos mínimos de segurança, como criptografia ativa, presença de agentes corporativos, conformidade de políticas, chaves de segurança e comunicação adequada com os serviços de gestão, o dispositivo é reintegrado ao ambiente produtivo.

A arquitetura adota princípios de Confiança Zero (Zero Trust), garantindo que a conformidade seja validada antes de qualquer concessão de acesso à rede produtiva. O EDR implementado atua com análise comportamental, auxiliando na detecção de possíveis anomalias residuais de persistência do malware, enquanto os eventos de restauração geram logs centralizados para análise forense e revisão pós-incidente.

A integridade dos artefatos restaurados também pode ser validada por meio de hashes SHA-256, permitindo comparar imagens, arquivos críticos e pacotes de configuração com versões previamente homologadas. Essa validação contribui para identificar alterações não autorizadas nos componentes verificados. No entanto, a ausência de persistência maliciosa deve ser confirmada por controles complementares, como varredura por EDR/antimalware, análise de serviços ativos, tarefas agendadas, registros de inicialização, logs de segurança e validação de conformidade antes da reintegração definitiva do dispositivo à rede produtiva.

8. DISCUSSÃO: GESTÃO DE RECURSOS HUMANOS

A eficácia do Plano de Recuperação de Desastres (DRP) na MVDP Tech fundamenta-se na integração entre a automação técnica e a especialização do capital humano. Para assegurar a agilidade necessária em infraestruturas logísticas críticas, a organização adota um modelo de operação enxuta, composto por uma equipe de três técnicos especialistas, cuja produtividade é maximizada pela redução de tarefas manuais repetitivas.

Diferente dos métodos convencionais de configuração individualizada, a estratégia utiliza o provisionamento em massa por meio de imagens padronizadas (Golden Images). Este modelo de "reentrega controlada" permite a restauração simultânea de múltiplos ativos, garantindo que o RTO de 30 minutos seja respeitado sem comprometer a padronização de segurança de cada dispositivo.

A resiliência operacional é reforçada por dois pilares fundamentais de governança: observabilidade estratégica e gestão do conhecimento. A política de cross-training e a realização periódica de exercícios de simulação asseguram que o conhecimento crítico não esteja centralizado em um único indivíduo.

9. CONCLUSÃO

O presente estudo demonstrou que a resiliência cibernética moderna em ambientes de alta criticidade depende da integração estratégica entre diretrizes normativas, como as publicações do NIST, automação técnica e especialização operacional. A implementação de Golden Images e unidades offline permitiu alcançar RTOs inferiores a 30 minutos, validando a eficácia do modelo proposto para grandes ecossistemas tecnológicos em que o impacto de indisponibilidades em cascata pode ser sistêmico e irreversível.

Conclui-se que a efetividade de um Plano de Recuperação de Desastres (DRP) vai além da continuidade operacional imediata, fundamentando-se na capacidade de restauração segura com previsibilidade e rastreabilidade. Em cenários com alta dependência de dispositivos finais, a combinação de padronização de imagens, segregação de rede e automação de configuração estabelece um modelo de

recuperação consistente e escalável, reduzindo drasticamente a variabilidade operacional, aumentando a previsibilidade técnica entre execuções e contribuindo para mitigar o risco de reinfecções.

Além disso, o trabalho evidencia que métricas como RTO, RPO e MTTR devem ser tratadas como indicadores de gestão baseada em evidências, sustentados por simulações recorrentes que tornam visíveis gargalos operacionais e dependências críticas.

10. LIMITAÇÕES E TRABALHOS FUTUROS

Como limitações, destaca-se que o estudo foi conduzido com base em um exercício prático controlado e em um conjunto de 30 ativos, o que pode não representar toda a variabilidade de hardware, perfis de uso e condições de rede existentes em ambientes distribuídos em múltiplos Centros de Distribuição. Além disso, o recorte priorizou cenários de ransomware e recuperação de endpoints, não abrangendo, em profundidade, eventos como indisponibilidade prolongada de links, falhas elétricas em larga escala, comprometimento de credenciais privilegiadas ou ataques à cadeia de suprimentos de software.

Como trabalhos futuros, recomenda-se expandir os testes para múltiplos CDs simultaneamente e avaliar a resiliência do tráfego de comunicação com a nuvem por meio de arquiteturas como SD-WAN. Também se recomenda aprofundar a análise de recuperação de credenciais privilegiadas, integração com plataformas SOAR, validação automatizada de conformidade e testes de recuperação sob cenários de indisponibilidade parcial ou total de conectividade externa.

REFERÊNCIAS

ALHAZMI, Omar H.; MALAIYA, Yashwant K. Application of vulnerability discovery models to major operating systems. **IEEE Transactions on Reliability**, v. 57, n. 1, p. 14-22, 2008. DOI: 10.1109/TR.2008.916872.

ALKHALEEL, Basem A. Machine learning applications in the resilience of interdependent critical infrastructure systems: a systematic literature review. **International Journal of Critical Infrastructure Protection**, v. 44, p. 1-15, 2024. DOI: 10.1016/j.ijcip.2023.100646.

CERULLO, Virginia; CERULLO, Michael J. Business continuity planning: a comprehensive approach. **Information Systems Management**, v. 21, n. 3, p. 70-78, 2004. DOI: 10.1201/1078/44432.21.3.20040601/82480.11.

CIS - CENTER FOR INTERNET SECURITY. **CIS Critical Security Controls Version 8**. East Greenbush: CIS, 2021.
CIS - CENTER FOR INTERNET SECURITY. **CIS Benchmarks**. East Greenbush: CIS, [s. d.]. Disponível em: https://www.cisecurity.org/cis-benchmarks. Acesso em: 10 maio 2026.

CRESWELL, John W.; CRESWELL, J. David. **Projeto de pesquisa**: métodos qualitativo, quantitativo e misto. 5. ed. Porto Alegre: Penso, 2021.

CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY. **StopRansomware Guide**. CISA, 2023. Disponível em: https://www.cisa.gov/stopransomware. Acesso em: 10 maio 2026.

FERNANDES, Aguinaldo Aragon; ABREU, Vladimir Ferraz de. **Implantando a Governança de TI**: da estratégia à gestão dos processos e serviços. 4. ed. Rio de Janeiro: Brasport, 2014.

FONTES, Edison Luiz Gonçalves. **Segurança da Informação**. São Paulo: Saraiva, 2017.

IDC; ZERTO. **The State of Disaster Recovery and Cyber-Recovery, 2024-2025**: Factoring in AI. Framingham: IDC, 2024. Disponível em: https://www.idc.com/showcase/the-state-of-disaster-recovery-and-cyber-recovery-2024-2025-factoring-in-ai/. Acesso em: 10 maio 2026.

LOHMER, Jacob; BUGERT, Nils; LASCH, Rainer. Analysis of resilience strategies and ripple effect in blockchain-coordinated supply chains: an agent-based simulation study. **International Journal of Production Economics**, v. 228, p. 107882, 2020. DOI: 10.1016/j.ijpe.2020.107882.

MICROSOFT. **Get started with the Microsoft Deployment Toolkit**. Microsoft Learn, [s. d.]. Disponível em: https://learn.microsoft.com/en-us/windows/deployment/deploy-windows-mdt/get-started-with-the-microsoft-deployment-toolkit. Acesso em: 10 maio 2026.

NIST - NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **Contingency Planning Guide for Federal Information Systems**. NIST Special Publication 800-34 Revision 1. Gaithersburg: NIST, 2010.

NIST - NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **Computer Security Incident Handling Guide**. NIST Special Publication 800-61 Revision 2. Gaithersburg: NIST, 2012.

NIST - NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **Data Integrity**: Recovering from Ransomware and Other Destructive Events. NIST Special Publication 1800-11. Gaithersburg: NIST, 2017.

NIST - NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **Security and Privacy Controls for Information Systems and Organizations**. NIST Special Publication 800-53 Revision 5. Gaithersburg: NIST, 2020a.

NIST - NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **Zero Trust Architecture**. NIST Special Publication 800-207. Gaithersburg: NIST, 2020b.

NIST - NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **Developing Cyber-Resilient Systems**: A Systems Security Engineering Approach. NIST Special Publication 800-160 Volume 2 Revision 1. Gaithersburg: NIST, 2021.

RAVAL, K. J. *et al*. A survey on safeguarding critical infrastructures: attacks, AI security, and future directions. **International Journal of Critical Infrastructure Protection**, v. 44, p. 1-22, 2024. DOI: 10.1016/j.ijcip.2023.100647.

SAHEBJAMNIA, Navid; TORABI, S. A.; MANSOURI, S. A. Integrated business continuity and disaster recovery planning: towards organizational resilience. **European Journal of Operational Research**, v. 242, n. 1, p. 261-273, 2015. DOI: 10.1016/j.ejor.2014.09.055.

WALLACE, Michael; WEBBER, Lawrence. **The Disaster Recovery Handbook**: a step-by-step plan to ensure business continuity and protect vital operations, facilities, and assets. 3. ed. New York: AMACOM, 2017.

YIN, Robert K. **Estudo de caso**: planejamento e métodos. 5. ed. Porto Alegre: Bookman, 2015.