

Conteúdo patrocinado | White paper

A disposição de ativos de TI está quebrada — e isso está custando caro

Um chamado para reinventar o ITAD como foco estratégico, não apenas um item de checklist operacional



CIO

Patrocínio



As organizações gerenciam rotineiramente vários tipos de hardware em data centers, ambientes de usuários finais e operações globais, o que significa que precisam aposentar com segurança esses ativos quando chega a hora. Ainda assim, embora seja crítico para reduzir riscos e manter a conformidade, o IT asset disposition (ITAD) continua sendo uma reflexão tardia para muitas empresas.

Apesar do aumento da consciência sobre os riscos de dados envolvidos, profissionais de TI ainda encaram o ITAD como uma tarefa logística de fim de vida, e não como uma função central de segurança. Como resultado, as abordagens são fragmentadas, subfinanciadas e inconsistentes — abrindo lacunas que representam riscos significativos.

Este white paper apresenta novos achados de pesquisa que ilustram essa desconexão e defende a elevação do ITAD a um imperativo estratégico que reduz riscos, impulsiona melhorias operacionais e gera benefícios financeiros.

Consciência é alta, mas a execução fica aquém

A maioria dos tomadores de decisão de TI entende que dispositivos em fim de vida representam riscos de segurança de dados e de conformidade. Em uma pesquisa recente do Foundry MarketPulse, 56% apontaram a exposição de dados no fim de vida como uma das principais preocupações, e 64% informaram oferecer treinamentos regulares relacionados a ITAD.



Na prática, porém, poucos têm processos padronizados, titularidade clara ou orçamento suficiente. Uma das principais razões é que o ITAD costuma ser classificado de forma incorreta — atribuído a facilities ou compras em vez de riscos ou segurança — e tratado como uma questão de ativo físico, não como uma prioridade do ciclo de vida dos dados.

Essa mentalidade, reforçada por hábitos desatualizados e pela falta de alinhamento interno, leva a execução inconsistente e subfinanciamento. Além disso, enquanto os tomadores de decisão

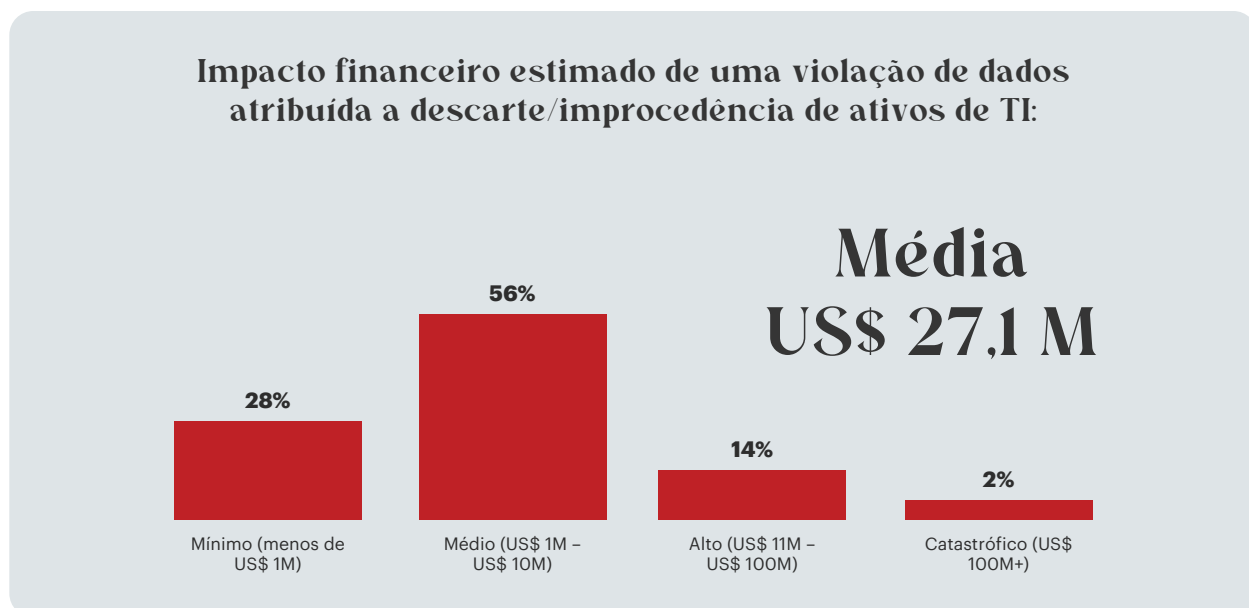
concentram recursos em ameaças ativas (como malware e intrusões), acabam negligenciando os riscos latentes associados ao manuseio inadequado de dispositivos. Como o ITAD geralmente ocorre no fim da vida do dispositivo, ele tende a não receber o mesmo nível de investimento que a infraestrutura ativa. A pesquisa mostrou que a empresa média aloca apenas 5% do orçamento de segurança para ITAD, e quase dois terços gastam menos do que isso.

Resultado final: Apesar de seu papel em proteger dados sensíveis e assegurar conformidade, o ITAD permanece subpriorizado nas operações de TI, com a maioria das organizações deixando de tratá-lo como prioridade de negócio e perdendo benefícios financeiros que poderiam compensar custos com práticas aprimoradas.

Para fechar a lacuna entre risco e recursos, as organizações precisam formalizar programas de ITAD como parte de suas estratégias de conformidade e segurança. Isso inclui atribuir titularidade, alinhar orçamentos e padronizar políticas entre unidades de negócio e geografias. Também exige envolver um conjunto mais amplo de stakeholders. O ITAD toca várias funções — TI, segurança, compras, finanças e sustentabilidade — todas interessadas em reduzir risco, gerir custos e apoiar metas de ESG. Quando essas equipes se coordenam por meio de um programa centralizado, conseguem melhorar a proteção de dados, reduzir gastos desnecessários e recuperar valor residual de ativos aposentados.

Riscos do ITAD inadequado

O ITAD inadequado expõe empresas a riscos significativos, incluindo vazamentos de dados, perda de confiança de clientes, escrutínio regulatório, multas e danos duradouros à marca. Segundo os respondentes, o custo médio de uma violação ligada a ITAD inadequado é de US\$ 27,1 milhões.





Para ilustrar, considere este caso real: um grande banco global contratou um terceiro para aposentar dispositivos de TI contendo informações pessoalmente identificáveis. O fornecedor não sanitizou adequadamente os dispositivos nem forneceu certificados de destruição para todos os ativos, e os equipamentos foram posteriormente revendidos online. O banco foi considerado em violação de regulamentos de proteção de dados e responsabilizado pelo manuseio inadequado do fornecedor. A violação ganhou manchetes mundiais, prejudicou a reputação e resultou em multas federais de dezenas de milhões de dólares.

A cadeia de custódia fraca e a falta de certificação que levaram a esse incidente são vulnerabilidades comuns em ITAD. Outros pontos fracos incluem:

- Execução inconsistente de políticas de ITAD e gestão de múltiplos fornecedores em ambientes distribuídos;
- Dependência de terceiros sem credenciais apropriadas;
- Lacunas de documentação e trilhas de auditoria;
- Métodos de sanitização de dados que não atendem a padrões do setor (por exemplo, NIST 800-88).

As organizações devem encarar o ITAD como componente central de sua postura de segurança de dados, especialmente com o aumento do escrutínio em torno da proteção de dados global e da conformidade com regulamentos como HIPAA e GDPR. Apesar dessas vulnerabilidades e de incidentes de grande repercussão, muitas empresas subestimam seu nível de risco: 56% disseram que o risco de exposição devido a lacunas de ITAD é baixo, enquanto 44% admitiram exposição de risco pelo menos moderada — sinal de excesso de confiança, padrões inconsistentes ou ambos.

Abordagem fragmentada aumenta o risco

O surgimento de organizações distribuídas, forças de trabalho remotas e novos estilos de trabalho criou novos desafios. Usuários finais podem estar em vários locais, viajar com frequência e ter múltiplos dispositivos, o que complica a gestão de ativos de hardware.

Nesses cenários, muitas organizações adotam múltiplas abordagens de ITAD e até dependem de vários fornecedores em regiões e unidades de negócio diferentes, em nome da conveniência e da redução de custos. Mas essa estratégia pode resultar em aplicação inconsistente, falhas de comunicação e baixa visibilidade.

Sem controle centralizado, é difícil garantir que as equipes sigam a política e destruam dados com segurança. Isso também complica a prontidão para auditorias; 24% dos respondentes disseram que sua organização precisaria de pelo menos um mês para se preparar para uma auditoria.

Ao unificar processos de ITAD entre regiões e unidades e padronizar em um único provedor, as empresas podem assegurar conformidade global consistente, reduzir riscos relacionados a fornecedores e melhorar relatórios e controle da cadeia de custódia. Para isso, é preciso designar formalmente o ITAD como parte das estratégias de segurança e conformidade, reconhecê-lo como função central de gestão de dados e criar programas com políticas dedicadas, supervisão e responsabilização.

A titularidade desses programas geralmente fica com TI, mas requer coordenação e comunicação regular com outros stakeholders-chave, incluindo ESG, compras, segurança e finanças. Eliminar silos entre esses departamentos fortalece a governança, melhora o alinhamento e permite decisões mais informadas sobre a gestão de ativos em fim de vida.



O business case do ITAD

Quando bem implementado, o ITAD traz benefícios que vão além da redução de risco. Ele pode gerar valor tangível em várias áreas do negócio.

Exemplo: processos de ITAD seguros minimizam e-waste e reduzem emissões de carbono ao incentivar acondicionamento e reutilização de dispositivos como alternativas de maior valor em relação à reciclagem de e-waste — contribuindo mais para metas de ESG. Muitos dispositivos ainda têm valor financeiro ao fim do uso, que pode ser recuperado por meio de revenda ou doação após sanitização adequada de dados. Isso reduz o TCO (às vezes compensando de forma significativa os custos do fornecedor de ITAD), enquanto reforça responsabilidade corporativa e iniciativas de impacto social. Além disso, estratégias centralizadas de ITAD reduzem a complexidade interna, o que melhora a eficiência.

Apesar dos benefícios, organizações podem ter dificuldade em quantificar e comunicar o valor completo de seus programas de ITAD. Métricas/KPIs a considerar:

- Prevenção de violação de dados e multas por não conformidade;
- Redução de custos de compras de TI devido a melhor recuperação e redistribuição de dispositivos;
- Evitação de multas por atraso na devolução de leasing;
- Desvio de aterro e redução de emissões de carbono, comparando reuso com reciclagem;
- Redução de fornecedores e ganhos de eficiência com gestão consolidada.

Monitorar essas métricas ajuda a construir um business case robusto para ITAD e demonstra como ele apoia outras metas do negócio — combatendo a ideia de que ITAD é apenas uma tarefa logística, não uma iniciativa estratégica como outras de segurança e conformidade.

Esse argumento — re enquadrar o ITAD — deve ressoar com as preocupações de várias equipes:

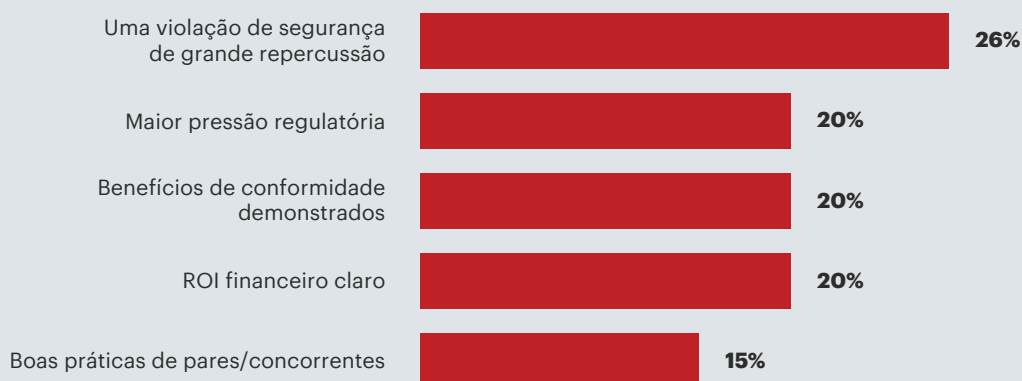
- **Risco e segurança:** destruição segura de dados e prevenção de violações;
- **Finanças e compras:** ROI e otimização de custos;
- **TI:** supervisão centralizada e menos atrito na gestão de ativos;
- **ESG:** impactos ambientais mensuráveis.

Apoiar esses argumentos com dados precisos e atualizados é crítico para transformar o ITAD em uma função estratégica de negócios.

Top drivers of ITAD investment

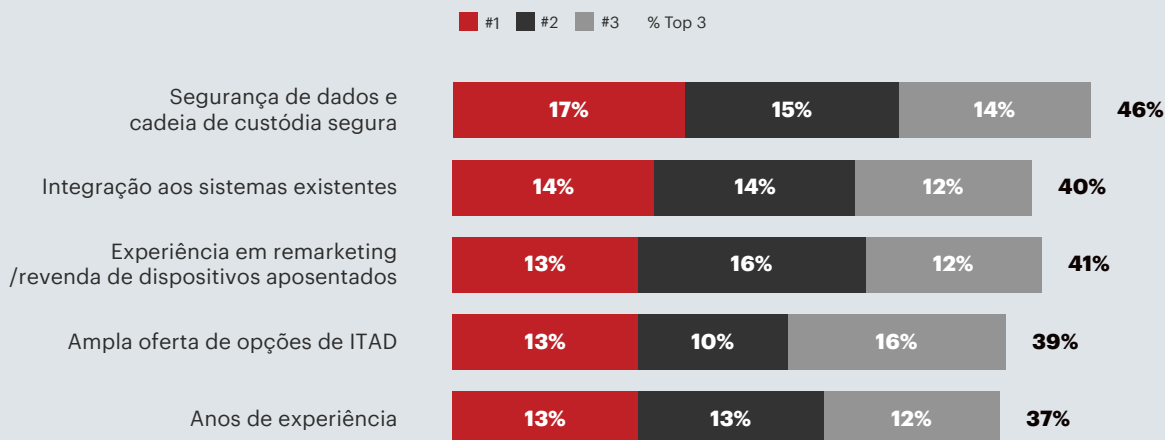
Embora o business case seja amplo, segurança continua sendo o principal motivador de investimento. Uma violação de grande repercussão é o gatilho nº 1 para gestão do ciclo de vida de ativos de TI: 26% dos respondentes a identificaram como disparador. Razões financeiras e regulatórias são quase tão influentes: 20% citaram maior pressão regulatória, ROI financeiro claro e benefícios comprovados de conformidade como vetores.

Fatores que mais aumentariam o investimento em ITAD:



Segurança também é o principal critério na seleção de fornecedores de ITAD. Ao listar os três critérios mais importantes, 46% incluíram segurança de dados e cadeia de custódia segura.

Top 3 critérios na escolha de um fornecedor de ITAD





O caminho adiante

Para organizações que desejam elevar o papel do ITAD, o caminho começa pela formalização. Isso significa priorizar explicitamente o ITAD como componente central das estratégias de segurança de dados e conformidade, superando processos ad hoc e atribuindo titularidade clara para que receba a atenção e o suporte de política necessários.

O passo seguinte é unificar a supervisão do ITAD entre regiões, departamentos e tipos de ativos — permitindo aplicação consistente de políticas, melhor visibilidade e coordenação interna mais fluida. Processos e documentação padronizados ajudam as equipes a responder mais rápido e com confiança a auditorias, reduzindo o risco de lacunas na destruição de dados ou no rastreamento de conformidade. As organizações também devem assegurar colaboração regular entre os donos do ITAD e áreas adjacentes como conformidade, finanças, compras e ESG. Essas conversas interfuncionais são essenciais para alinhar metas, identificar prioridades sobrepostas e maximizar valor.

A seleção do fornecedor é igualmente importante. Organizações que trabalham com múltiplos provedores de ITAD acabam descobrindo que cada um possui padrões, certificações e capacidades diferentes, resultando em uma abordagem fragmentada que aumenta a complexidade e prejudica a consistência. Ao consolidar o ITAD com um único parceiro certificado, que ofereça cadeia de custódia segura, gestão centralizada do programa e relatórios robustos, as organizações podem proteger melhor os dados, simplificar operações e gerar insights de desempenho mais claros. O parceiro certo também deve apoiar metas de sustentabilidade por meio de reuso ambientalmente responsável de TI e reciclagem de e-waste, além de fornecer relatórios detalhados que quantifiquem redução de emissões, desvio de aterro e recuperação de valor.

Com esses elementos, o ITAD pode evoluir para uma função totalmente integrada que protege dados, apoia prioridades de ESG e contribui para um desempenho de negócios mais forte.

Este estudo de pesquisa personalizado foi encomendado pela Iron Mountain Asset Lifecycle Management. Para saber como a Iron Mountain pode ajudar sua organização a mitigar riscos e transformar o ITAD em uma vantagem estratégica, visite www.ironmountain.com/ALM