DATA ERASURE · DATA GOVERNANCE · COMPLIANCE · PRIVACY

WHITEPAPER · 2025

SOBREVIVER E PROSPERAR NA ERA DA PRIVACIDADE

Governança de Dados com Overty

Overty®

overtytech.com · Data Erasure & Governance

CONTEÚDO

Governança de Dados com Overty

$4.44M
COSTO PROMEDIO
custo médio de uma violação de dados IBM 2025

240+
DÍAS
tempo de detecção e contenção

100%
CERTIFICADO
apagamento auditado independentemente

01

Introdução

Por que o apagamento de dados importa?

Vivemos em um mundo onde a gestão de dados é estratégica. As organizações geram, coletam e processam enormes quantidades de informação: desde identificadores pessoais e registros financeiros até comunicações eletrônicas e dados sensíveis de clientes e funcionários. Contudo, nem toda essa informação tem valor permanente para o negócio ou uma finalidade legal que justifique sua conservação indefinida.

Quando dados que não deveriam mais existir continuam armazenados, não apenas desperdiçam recursos tecnológicos, mas também aumentam o risco de exposição indesejada. Essa acumulação de informações desnecessárias faz com que cada violação ou acesso não autorizado possa ter um impacto mais amplo e custoso para a organização.

O risco é quantificável e crescente

O **IBM Cost of a Data Breach Report 2025** relata que o custo médio global de uma violação de dados é de **USD $4,44 milhões** por incidente. Este custo inclui:

— Custos de resposta imediata

— Investigações forenses

— Multas regulatórias

— Perda de receita e clientes

— Danos reputacionais

> ■ **Dado chave**
>
> Os tempos de detecção e contenção de violações frequentemente excedem 240 dias, multiplicando o dano total do incidente.
> Quanto mais dados uma empresa retém, maior é sua superfície de ataque.

Além da segurança: privacidade e confiança

Eliminar dados desnecessários é uma **medida de respeito à privacidade das pessoas**. Um banco de dados saturado de informações obsoletas pode ser explorado para roubo de identidade, fraude ou phishing direcionado, e aumenta a probabilidade de exposição de dados pessoais sensíveis.

Eliminar dados desnecessários **reduz a "pegada de dados" da organização**, habilitando uma postura de privacidade mais sólida, confiável e defensável perante reguladores.

Conclusão da seção: O apagamento seguro de dados reduz de forma real e mensurável o risco de violações custosas, otimiza a infraestrutura e reforça a confiança de clientes, parceiros e auditores.

02

Estado Atual

Ferramentas sem governança

Em muitas organizações existe uma **contradição crítica**: possuem licenças de software para apagar dados, mas **não têm uma abordagem estruturada de gestão do apagamento** como parte de sua governança de dados. Essa lacuna entre tecnologia e processo tem consequências importantes.

O que está realmente acontecendo?

Embora as ferramentas de apagamento possam eliminar informações individualmente, não resolvem por si só os desafios organizacionais:

- **Sem processos formais documentados** que estabeleçam como e quando apagar cada tipo de dado.
- **Sem políticas de retenção aprovadas** com regras claras baseadas em riscos e regulações.
- **Sem integração com processos críticos de negócio** como backups, leasing de equipamentos ou desligamento de funcionários.
- **Sem matriz de retenção** que atribua prazos por tipo de informação e marco regulatório.
- **Sem rastreabilidade centralizada** nem evidência auditável que respaldem decisões de eliminação.

Consequências da lacuna estrutural

O apagamento ocorre de forma reativa, sem critérios formais.
Não há evidência documentada para auditorias ou reguladores.
Princípios de minimização e qualidade do dado são descumpridos.
O risco cresce silenciosamente a cada dia.

03

Marco Regulatório

O imperativo de conformidade

O panorama regulatório global exige não apenas proteger os dados, mas também gerenciar seu ciclo de vida completo — incluindo sua eliminação oportuna e verificável. As organizações sem processos formais de apagamento enfrentam sanções crescentes.

GDPR (Europa)

Exige o "direito ao apagamento" e a minimização de dados. Reter informações sem finalidade legítima viola o princípio de limitação de armazenamento.

ISO/IEC 27001

Exige controles formais sobre o ciclo de vida do ativo de informação e o descarte seguro de mídias e equipamentos. Controle 8.10 do Anexo A.

PCI-DSS

Exige que os dados do portador de cartão sejam retidos apenas quando estritamente necessário e eliminados de forma segura e verificável. Requisitos 3.1 e 3.2.

HIPAA (EUA)

Estabelece requisitos específicos para o descarte de informações de saúde protegidas, tanto em formato físico quanto digital.

LGPD (Brasil)

Prevê o direito de eliminação e obriga a suprimir dados quando cumprida a finalidade para a qual foram coletados.

■ A diferença crítica

Cumprir não basta — é preciso DEMONSTRAR a conformidade.
Sem evidência documentada de eliminação, não há conformidade real.
Os reguladores exigem rastreabilidade, não apenas boas intenções.

04

Os Riscos Reais

De não governar o ciclo de vida do dado

Cada arquivo esquecido, cada backup histórico sem depuração, cada dispositivo reatribuído sem controle formal é uma possível fonte de exposição. Não governar o apagamento não é uma omissão menor: **é um risco estrutural**.

4.1 Privacidade comprometida

■ Amplia a superfície de ataque

Más datos almacenados significan más vectores potenciales de acceso. Os atacantes não distinguem entre dados "ativos" e dados "esquecidos".

■ Amplifica a exposição em violações

Quando ocorre um incidente, o impacto depende diretamente do volume e sensibilidade das informações comprometidas. Reter dados sem finalidade amplifica o dano.

■ Pode gerar sanções regulatórias

As leis de proteção de dados exigem reter informações apenas pelo tempo necessário. Manter dados sem justificativa pode constituir descumprimento.

4.2 Custos financeiros reais

O custo médio de uma violação alcança **USD $4,44 milhões**. Com governança inadequada, o impacto se amplifica pelo maior volume de dados comprometidos, escopo regulatório adicional, complexidade forense e mais notificações obrigatórias.

■ Serviços forenses e jurídicos

■ Perda de confiança dos clientes

■ Cancelamento de contratos

■ Aumento nos prêmios de ciberseguro

■ Danos reputacionais de longo prazo

> **■ O risco silencioso**
>
> O risco mais silencioso é NÃO ELIMINAR dados quando necessário.
> A acumulação indiscriminada de informações não é força digital.
> É vulnerabilidade acumulada — visível para os atacantes.

05

A Solução Overty

Governança, automação e rastreabilidade

A maioria das organizações já possui ferramentas de apagamento. O que não têm é **governança**. A Overty propõe uma mudança de paradigma: do apagamento reativo ao **apagamento governado, automatizado e auditável**.

Não se trata apenas de eliminar dados. Trata-se de transformar a eliminação em um processo corporativo formal, alinhado à regulação, ao risco e à estratégia empresarial.

O que diferencia a Overty?

✔ Política corporativa de retención y eliminación

Desenho e implementação de diretrizes formais alinhadas à regulação e às melhores práticas internacionais.

✔ Matriz de retención por tipo de dato

Definição clara do que se retém, por quanto tempo e sob qual fundamento legal ou regulatório.

✔ Integración con procesos críticos de negocio

Backup, leasing, renovação tecnológica, migrações e desligamentos deixam de ser pontos cegos.

✔ Trazabilidad centralizada y reportes auditables

Evidência consolidada e verificável, pronta para auditorias internas ou regulatórias.

✔ Evidencia certificada de eliminación

Suporte documental alinhado ao NIST 800-88, DoD 5220.22-M, ISO 27001, PCI-DSS e GDPR.

> ■ **A proposta de valor**
>
> A Overty não apenas executa o apagamento.
> Transforma-o em um controle corporativo defensável.
> Governança estruturada + automação + rastreabilidade
> alinhada a marcos regulatórios internacionais.

06

Conformidade Regulatória

Overty como habilitador de evidência

A diferença entre cumprir e demonstrar conformidade é crítica. A falta de evidência documentada pode gerar observações, achados ou sanções nos marcos regulatórios mais exigentes.

ISO/IEC 27001

Exige controles formais sobre o ciclo de vida do ativo. A Overty gera evidência alinhada ao Anexo A, Controle 8.10.

PCI-DSS

Exige eliminação segura e verificável de dados sensíveis. A Overty atende aos requisitos 3.1 e 3.2.

LGPD / ANPD

Exige gestão de riscos tecnológicos e evidência de implementação de controles de proteção de dados.

GDPR / LGPD

O apagamento certificado da Overty suporta o direito ao apagamento e o princípio de minimização em ambos os marcos.

Sem processo, não há controle. Sem evidência, não há conformidade. A Overty fecha a lacuna entre a ferramenta técnica e o processo corporativo, integrando governança, automação e rastreabilidade em um único marco operacional.

07

Conclusão

A privacidade como vantagem competitiva

O dado já não é apenas um ativo tecnológico ou financeiro. É um ativo reputacional, regulatório e estratégico. As organizações são responsáveis por gerenciar o ciclo de vida completo de suas informações, incluindo sua eliminação oportuna e verificável.

Em um ambiente onde as regulações são cada vez mais rígidas, as violações mais frequentes e custosas, e os clientes exigem maior transparência, a privacidade se torna um elemento de **confiança empresarial** — não apenas de conformidade.

As organizações que governam o ciclo de vida do dado:

✔ Reduzem sua exposição a riscos legais e financeiros

✔ Diminuem o impacto potencial de incidentes de segurança

✔ Fortalecem sua postura perante auditorias e reguladores

✔ Geram credibilidade junto a clientes e investidores

✔ Transformam a privacidade em vantagem competitiva sustentável

■ O resultado

A Overty permite migrar de um apagamento informal e reativo para um modelo estruturado, automatizado e auditável, alinhado a marcos regulatórios internacionais.

Em um mercado onde a confiança é um ativo escasso, a governança do dado se torna vantagem competitiva.

Overty Corporation LLC · overtytech.com

Data Erasure · Data Governance · Compliance · Privacy