

XTRME IT



10 Erros

no backup do Microsoft 365
que comprometem a resiliência cibernética

XTR
FRAMEWORK

XTREME IT

10 Erros

no backup do Microsoft 365
que comprometem a resiliência cibernética



SOBRE A **Xtreme IT**



Somos referência no mercado Enterprise em proteção e resiliência de dados.



Garantimos conformidade e redução de riscos cibernéticos para os negócios, com base em normas internacionais.



Transformamos nossa experiência em método, o XTR Framework.

15

15 anos de atuação em centenas de projetos entregues com excelência.



Especialistas no uso de IA para proteger dados críticos e garantir continuidade de negócios.



Somos Trusted Advisor. Estamos ao lado dos nossos clientes em toda jornada.

5PB+

Mais de 5 Petabytes de dados críticos protegidos pela nossa metodologia.

35bi+

Mais de R\$ 35 Bilhões em negócios protegidos.

10 Erros no backup do M365

AVISOS LEGAIS

Este eBook foi elaborado com o objetivo de compartilhar boas práticas de backup e segurança da informação, em caráter educativo e informativo.

Direitos autorais e propriedade intelectual

O conteúdo, incluindo textos, imagens, exemplos e orientações é protegido por leis de direitos autorais. A reprodução, modificação ou distribuição não autorizada é proibida.

As marcas e nomes comerciais citados pertencem aos seus respectivos titulares e são mencionados apenas para fins ilustrativos e agradecimento, sem qualquer vínculo, endosso ou patrocínio.

Uso institucional e educativo

O conteúdo pode ser compartilhado digitalmente, desde que mantido na íntegra, com os devidos créditos e sem aproveitamento comercial direto.

Isenção de responsabilidade

As informações aqui contidas têm caráter meramente informativo. A Xtreme IT não se responsabiliza por eventuais perdas, danos ou prejuízos decorrentes do uso das orientações apresentadas.

O uso deste material é de responsabilidade exclusiva do leitor.

Contato para autorizações:

Para solicitações de uso, reprodução ou adaptação, entre em contato pelo e-mail contato@xtremeit.com.br.

Conteúdo

INTRODUÇÃO.....	pg 7
PANORAMA DO MERCADO.....	pg 14
OS 10 ERROS NO BACKUP DO M365.....	pg 20
QUANDO O BACKUP FALHA.....	pg 33
IMPACTOS TÉCNICOS E EXECUTIVOS.....	pg 38
TÉCNICAS DE RESILIÊNCIA CIBERNÉTICA.....	pg 42
XTREME IT & DRUVA.....	pg 49
SQUAD DATA GUARDIANS.....	pg 58
CAMINHO PRÁTICO DE ADOÇÃO.....	pg 62
REFERÊNCIAS BIBLIOGRÁFICAS.....	pg 67
CRÉDITOS.....	pg 68

10 ERROS NO BACKUP DO M365

INTRODUÇÃO





INTRODUÇÃO

Microsoft 365: O Desafio da Resiliência e do Compliance

O Microsoft 365 se tornou a espinha dorsal da colaboração corporativa moderna. No entanto, suas proteções nativas não foram projetadas para enfrentar o ritmo crescente dos ataques cibernéticos nem as exigências cada vez mais rigorosas de compliance.

A realidade atual demonstra que, mesmo com avanços em segurança, muitas empresas ainda não estão preparadas para recuperar seus dados com agilidade e confiança após um incidente. A diferença entre estar protegido e estar resiliente está na estratégia, não apenas na tecnologia.

Este guia revela as 10 falhas mais comuns que comprometem a resiliência cibernética e o compliance em organizações que utilizam Microsoft 365 e mostra como evitá-las por meio de um modelo moderno de Data Protection as a Service (DPaaS), que eleva a proteção de dados a um novo patamar de eficiência e confiabilidade.

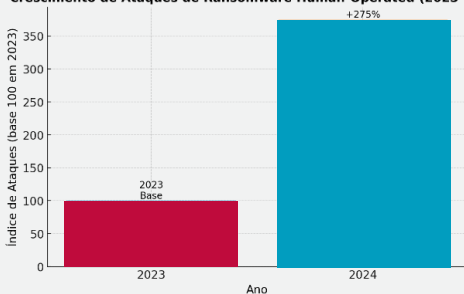
O cenário atual

Imagine o seguinte: Sua empresa depende do Microsoft 365 para reuniões, colaboração diária e armazenamento de documentos estratégicos, incluindo contratos e registros críticos.

Agora pense: E se, de repente, todos esses dados fossem sequestrados ou simplesmente apagados? Essa é a realidade de milhares de organizações hoje.

O Microsoft Digital Defense Report 2024 mostrou que os clientes da Microsoft enfrentam mais de 600 milhões de ataques cibernéticos todos os dias. Entre 2023 e 2024, os ataques de ransomware human-operated cresceram 275%, atingindo diretamente os dados críticos armazenados no M365.

Crescimento de Ataques de Ransomware Human-Operated (2023-2024)



Por que isso preocupa?

- **Compliance:** Reguladores como LGPD, Bacen, ANTT, ANS e ANVISA exigem retenção e relatórios auditáveis.
- **Continuidade:** A perda de dados pode interromper operações inteiras e custar milhões em receita.
- **Reputação:** Falhas corroem a confiança de clientes, investidores e parceiros.



- Retenção limitada: as políticas nativas do M365 são curtas e pouco granulares.
- Restauração complexa: Restore parcial e lento compromete a produtividade.
- Infraestrutura legada: soluções híbridas exigem appliances, licenças adicionais e administração constante.
- Baixo time-to-value: soluções fragmentadas demoram a entregar resultados e aumentam a carga operacional.

Complexidade crescente

Na América Latina, o IDC indica que menos de 30% dos workloads corporativos conseguem ser movidos entre provedores.

Essa baixa portabilidade cria uma dependência estrutural:

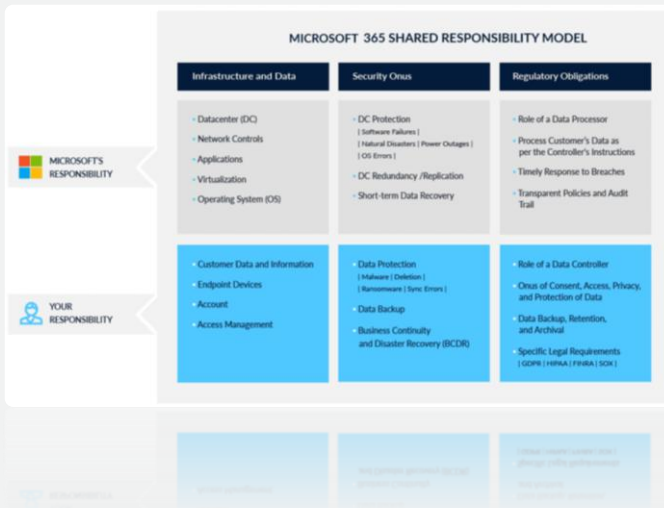
- Os dados ficam presos ao ecossistema da Microsoft.
- Exclusões, corrupções ou ataques só podem ser revertidos dentro das políticas nativas.
- E essas políticas não foram projetadas para requisitos mais rigorosos de compliance, auditoria ou recuperação avançada.

Em outras palavras: a baixa portabilidade na nuvem se traduz em limitação de controle e maior exposição ao risco.

Responsabilidade Compartilhada

O modelo de responsabilidade compartilhada da Microsoft é claro:

- Ela garante a disponibilidade da plataforma.
- Mas a responsabilidade pelos dados, identidades e configurações é sempre do cliente.



É por isso que tantas empresas descobrem tarde demais que "ter backup" não é o mesmo que estar resiliente.

O mercado entrou em uma fase de transição:

- As ameaças aumentam em volume e sofisticação.
- Os ambientes se tornam mais complexos com o modelo multicloud.
- Reguladores apertam o cerco e ampliam a cobrança por governança.

A responsabilidade final continua com a empresa, não com o provedor.



O Provedor de Nuvem é responsável pela segurança **DA** nuvem

O Cliente é totalmente responsável por proteger os dados na nuvem

O Provedor de Nuvem é responsável por proteger a infraestrutura da nuvem

Dúvidas gerais do mercado:

"Se pago pela nuvem, por que preciso me preocupar com segurança dos dados?"

- ***O pagamento pelo serviço de nuvem inclui a infraestrutura, mas a segurança é uma responsabilidade compartilhada.***

"Mas os dados estão na nuvem. Não deveria ser mais seguro?"

- ***Estar na nuvem não garante automaticamente mais segurança.***

"O Provedor de Nuvem já cuida obrigatoriamente do meu backup, certo?"

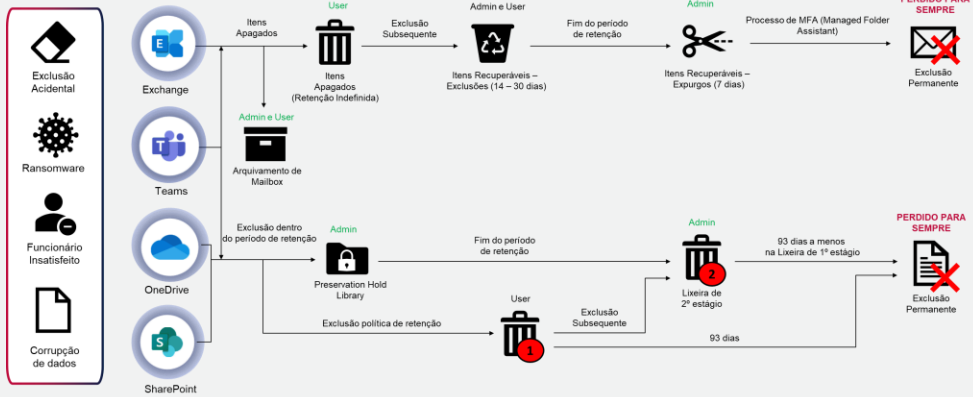
- ***A gestão do backup é uma responsabilidade do cliente.***



Backup nativo do M365 possui lacunas ocultas

- Dados ficam presos ao ecossistema Microsoft
- Exclusões acidentais, corrupções ou ataques só podem ser revertidos dentro das políticas nativas.
- Essas políticas não foram desenhadas para atender requisitos mais rigorosos de compliance, auditoria e recuperação avançada.

Múltiplas hipóteses, terminologias, localizações, personas, versões e ações



10 ERROS NO BACKUP DO M365

PANORAMA DO MERCADO





PANORAMA DO MERCADO

Nuvem: O campo de batalha digital

Segundo o Relatório de Investigação de Ameaças 2025 da CrowdStrike, houve um aumento de 136% nas intrusões em ambientes de nuvem no primeiro semestre de 2025, comparado a 2024. Destes casos, 40% foram atribuídos a adversários ligados ao China-Nexus, reforçando a crescente sofisticação e escala dos ataques.

A imensa concentração de dados sensíveis e as configurações incorretas frequentes tornam a nuvem um dos alvos mais atrativos do cenário atual. Grupos avançados exploram esse contexto com táticas inovadoras, como as redes ORB (Operational Relay Box), estruturas intermediárias usadas para ocultar comunicações entre sistemas comprometidos e os servidores de comando e controle (C2).

Em vez de o malware se conectar diretamente ao servidor do atacante (o que facilitaria sua detecção), ele trafega por uma cadeia de servidores proxy distribuídos, que funcionam como "zonas de salto" e dificultam a identificação da origem real do ataque.

Esses adversários coletam credenciais privilegiadas e migram lateralmente dentro dos ambientes de nuvem, acessando consoles administrativos e executando comandos em outras máquinas virtuais.

O grupo MURKY PANDA, por exemplo, explorou parceiros de confiança para invadir o Entra ID (antigo Azure AD) e obter acesso a aplicações corporativas na nuvem, incluindo e-mails e dados do SharePoint.

Em um cenário onde a nuvem é o novo campo de batalha digital, a proteção do M365 deixa de ser uma boa prática e se torna uma exigência estratégica.

Aumento de

136%

nas intrusões.

em ambientes de nuvem
no primeiro semestre de
2025, comparado a 2024.



MURKY PANDA

A pressão por resiliência de dados

O cenário global é claro: as empresas estão mais expostas do que nunca.

A transformação digital acelerou a migração para ambientes híbridos e SaaS, mas também ampliou a superfície de ataque e a complexidade de gestão de dados.

De acordo com o Dell Global Data Protection Index, mais de 90% das organizações já sofreram algum tipo de perda de dados ou interrupção operacional nos últimos anos.

Ainda assim, a maioria continua operando com múltiplas ferramentas de backup e planejando upgrades constantes, um sinal de que os modelos atuais não transmitem confiança nem previsibilidade.



**das organizações
já sofreram perda
de dados ou
interrupção nos
últimos anos.**

A verdade é simples: muitas empresas acreditam estar protegidas, mas operam sobre um terreno frágil.

Pressão regulatória

Além dos riscos operacionais e cibernéticos, cresce também a pressão das autoridades regulatórias.

Na América Latina, órgãos como BACEN, ANS, SUSEP, ANTT, ANVISA e a ANPD exigem registros íntegros, rastreabilidade dos dados e relatórios auditáveis.

No entanto, a realidade é que muitas empresas ainda dependem de processos manuais, com relatórios inconsistentes e sem trilhas completas de auditoria.

Essa falta de controle gera risco de multas, sanções e desgaste da credibilidade, especialmente em setores como finanças, saúde e seguros, onde a conformidade e a rastreabilidade de dados são obrigações legais e normativas.

Expectativas x Realidade

- Executivos colocam segurança e backup entre as três principais prioridades de investimento em TI.
- Mas, na prática, a confiança nos planos de recuperação é baixa: muitos CIOs e CISOs admitem que não sabem se seus restores funcionariam diante de um ataque real.
- Equipes técnicas se veem presas a ferramentas complexas e processos manuais, sem tempo para revisar políticas e testar cenários críticos.

Resultado: um grande gap entre expectativa e realidade - entre o que as empresas acreditam ter e o que realmente conseguem proteger.

- As ameaças são mais frequentes, sofisticadas e direcionadas.
- Ambientes SaaS e multicloud aumentam a dependência dos provedores.
- A pressão por compliance e transparência é crescente.
- Ferramentas legadas já não entregam a confiança necessária.

**Menos de 30%
dos workloads
corporativos
conseguem ser
movidos
facilmente entre
provedores.**



<30%

É nesse espaço (entre complexidade, conformidade e confiança) que surgem os erros mais comuns de proteção no Microsoft 365. E são eles que exploraremos no próximo capítulo.



**SEU PLANO DE RECUPERAÇÃO
FUNCIONARIA AMANHÃ?**

10 ERROS NO BACKUP DO M365

OS 10 ERROS NO BACKUP DO M365





OS 10 ERROS NO BACKUP DO M365

Por que ainda falhamos em proteger o M365?

Ter backup não é sinônimo de resiliência.

Muitas empresas acreditam estar protegidas apenas porque utilizam as políticas nativas do Microsoft 365 ou soluções tradicionais de backup.

A realidade é outra: continuam expostas a riscos que podem custar tempo, dinheiro e credibilidade.

O problema não está na ausência de backup, mas na ilusão de segurança.

Relatórios incompletos, restores lentos, dependência de infraestrutura legada e políticas desalinhadas de compliance formam um terreno fértil para incidentes.

E quando eles acontecem - seja por exclusão acidental, ataque de ransomware ou auditoria inesperada - essas fragilidades vêm à tona.

É nesse contexto que mapeamos os 10 erros mais comuns no backup do Microsoft 365, divididos em três grandes grupos:

- Riscos operacionais: quando a operação para.
- Riscos regulatórios: quando o problema vira sanção.
- Riscos estratégicos: quando a conta não fecha.

Conhecer esses erros é o primeiro passo para construir uma estratégia de proteção realmente resiliente.



Grupo 01

Riscos Operacionais

“ Quando a operação para ”

Mesmo com backup, muitas empresas descobrem tarde demais que operacionalmente não estão preparadas.

Os erros mais comuns estão relacionados a falhas de retenção, lentidão e infraestrutura obsoleta.

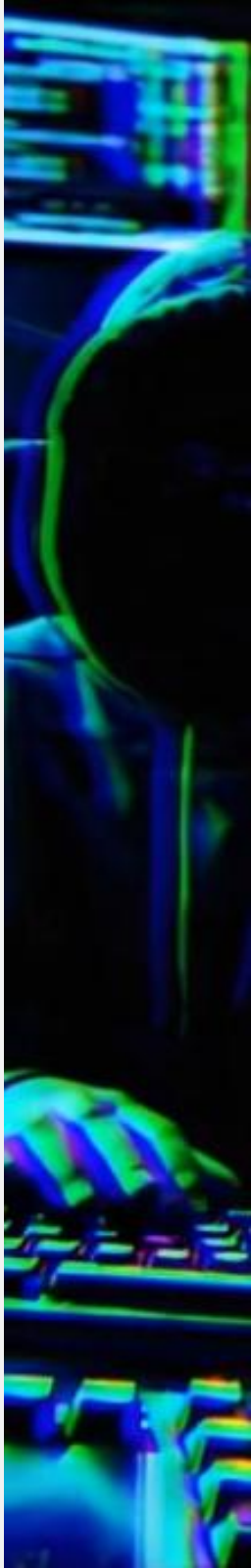
* Erro 01 Exclusões não cobertas

E-mails e arquivos críticos podem ser excluídos acidental ou intencionalmente.

As políticas nativas do Microsoft 365 oferecem apenas retenção limitada (30–90 dias), insuficiente para auditorias ou disputas legais.

Problema: quando a exclusão é percebida tardiamente, os dados podem já ter desaparecido sem possibilidade de recuperação.

Se um colaborador excluir dados-chave hoje, você teria como restaurar em minutos, em dias ou nunca?





Grupo 01

Riscos Operacionais

“ Quando a operação para ”

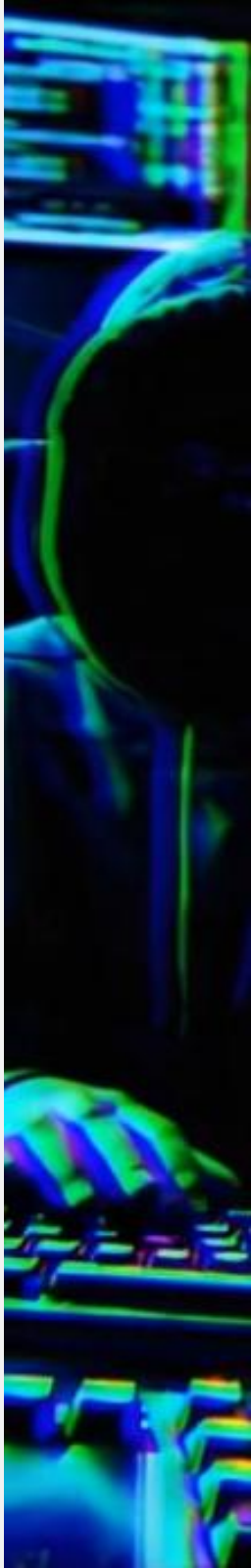
* Erro 02 Dados irrecuperáveis

A maior parte das perdas de dados irrecuperáveis não está relacionada à tecnologia, mas ao fator humano - exclusões acidentais, configurações incorretas ou processos manuais sem validação.

Segundo o estudo IDC Data Protection Survey 2025, o erro operacional foi citado por 46% dos entrevistados como uma das causas de perda definitiva de dados.

Outros fatores também aparecem com frequência, como falhas no intervalo entre backups (39%), que deixam dados desprotegidos entre execuções, e criptografia maliciosa por ransomware (36%), que inviabiliza a restauração segura.

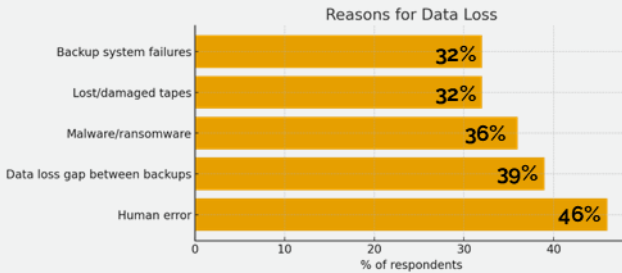
Além disso, falhas estruturais, como fitas danificadas (32%) ou erros no próprio sistema de backup (32%), continuam contribuindo para perdas definitivas, mostrando que a resiliência vai além de simplesmente ter uma cópia de segurança.





10 Erros no backup do M365

Qualidade extrema tem método – XTR Framework



A pesquisa permitiu múltiplas respostas, mostrando que a maioria dos incidentes envolve mais de uma falha combinada, humanas, técnicas e operacionais..

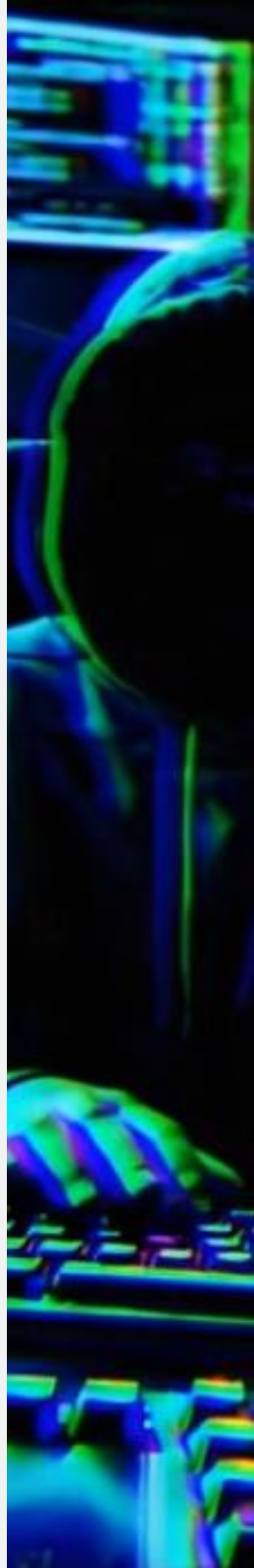
Ter backup não é suficiente.

Resiliência exige processo, automação, governança e validação contínua.

Quando a recuperação falha, a perda vai além dos arquivos: É tempo desperdiçado, retrabalho e impacto direto na continuidade do negócio.

46%

dos dados não recuperados são resultado de falha humana.





Grupo 01

Riscos Operacionais

“ Quando a operação para ”

* Erro 03 Dependência de infraestrutura legada

Soluções tradicionais ainda exigem licenciamento adicional, appliances, VMs ou serviços de integração.

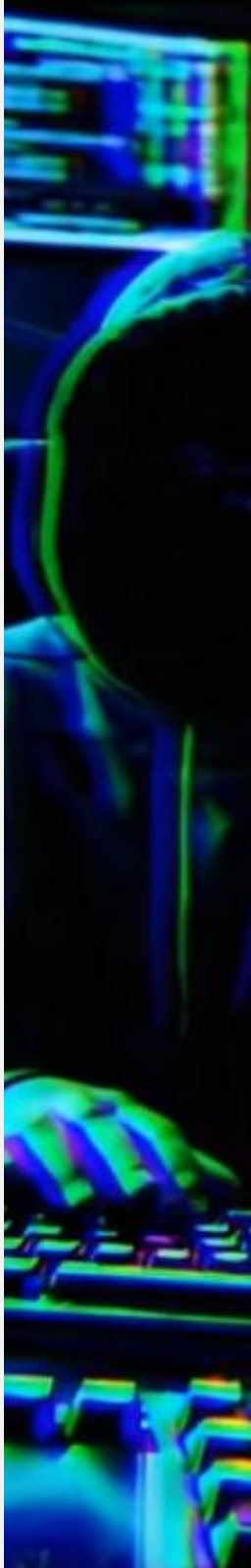
Cada componente extra adiciona custo, complexidade e pontos de falha.

Em momentos críticos - fechamento contábil, janelas de auditoria ou ataques de ransomware - isso se traduz em indisponibilidade e lentidão na resposta.

Impacto no negócio

- Improdutividade: equipes paradas ou refazendo tarefas.
- Perda de contratos: prazos descumpridos devido a dos indisponíveis.
- Custos ocultos: horas extras, retrabalho e upgrades não planejados.

A operação não falha por falta de backup, mas por falta de resiliência.





Grupo 02

Riscos Regulatórios

“ Quando o problema vira sanção ”

Compliance não é opcional.

Reguladores exigem retenções claras, trilhas de auditoria e relatórios verificáveis.

O problema é que muitas empresas descobrem falhas justamente durante uma auditoria ou litígio - quando já não há tempo para corrigir.

* Erro 04 Não alinhar backup às exigências de compliance

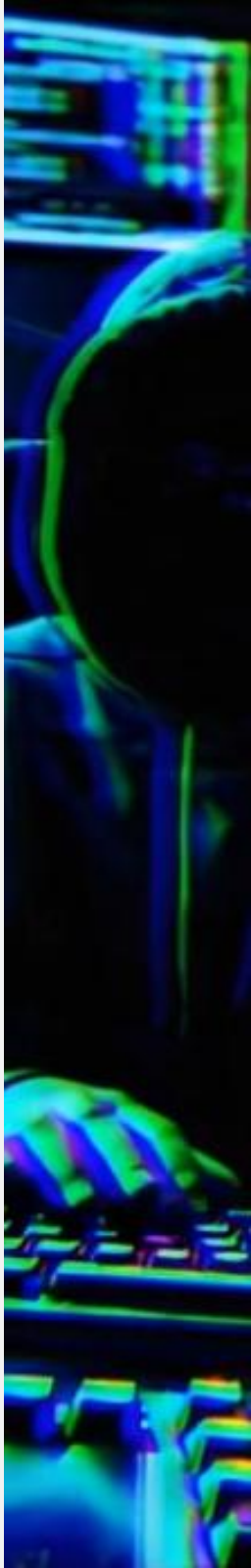
Os relatórios nativos do M365 não foram desenhados para cumprir requisitos regulatórios locais.

Resultado: informações incompletas ou não auditáveis.

Exemplo: imagine que sua empresa venha a ser envolvida em uma ação judicial por suposto descumprimento contratual ou má conduta.

Sem registros confiáveis, e-mails ou arquivos de anos atrás, a defesa se torna frágil.

A ausência de evidências pode levar à perda da ação, mesmo que a empresa estivesse de fato correta.





10 Erros no backup do M365

Qualidade extrema tem método – XTR Framework

Se amanhã sua empresa precisasse comprovar sua inocência em um processo sem provas, conseguiria restaurar e apresentar os e-mails corretos ou ficaria vulnerável?

* Erro 05 Relatórios inconsistentes

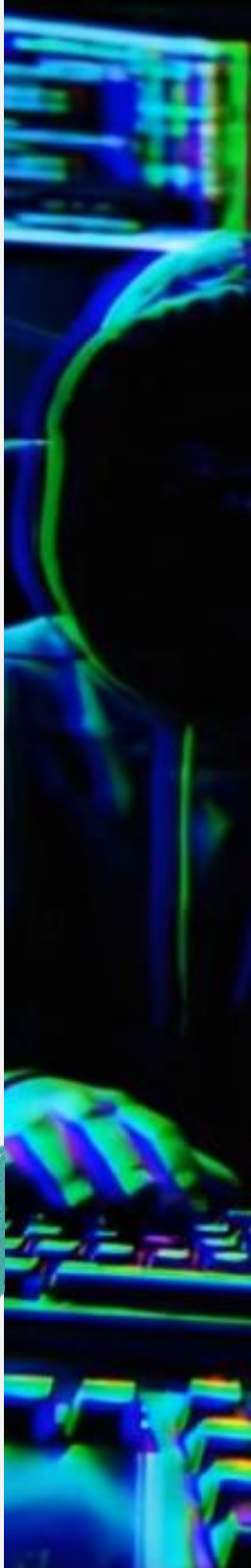
Sem automação, muitas empresas dependem de processos manuais e demorados.

A equipe de TI precisa extrair dados, consolidar planilhas e torcer para que passem por validação. Isso gera sobrecarga operacional e aumenta o risco de erro humano e não conformidade com auditoria.

Segundo o IDC, a governança de dados e a integração entre ambientes híbridos continuam sendo grandes desafios na América Latina.

Mais de 70% das empresas latino-americanas ainda lutam para consolidar governança e compliance em ambientes híbridos.

70%





Grupo 02

Riscos Regulatórios

“ Quando o problema vira sanção ”

* Erro 06 Falta de governança clara

Em muitas organizações, o backup é tratado como uma função sem dono: cada área define políticas sem visão centralizada.

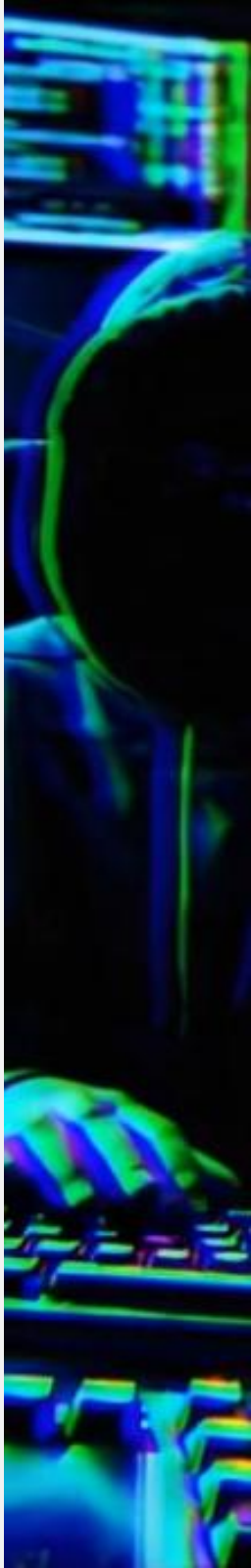
Em ambientes híbridos e multicloud, isso cria lacunas de proteção e políticas divergentes.

Consequência: não conformidade, risco de sanções e desgaste de credibilidade perante reguladores e conselhos.

Impacto no negócio

- Multas e sanções por falhas em auditorias.
- Limitações operacionais impostas por órgãos reguladores.
- Desgaste de reputação perante clientes, investidores e conselho.

Em outras palavras: um backup mal governado pode virar problema jurídico, e não apenas técnico.





Grupo 03

Riscos Estratégicos

“ Quando a conta não fecha ”

Ter backup não significa estar seguro. Muitas organizações que já investiram em soluções continuam com brechas invisíveis que só aparecem em auditorias, disputas contratuais ou crises.

E quando isso acontece, o impacto não é apenas técnico - é estratégico, comprometendo ROI, competitividade e confiança do mercado.

A seguir, exploramos alguns dos erros mais comuns que expõem essas fragilidades e mostram por que depender apenas de soluções nativas ou fragmentadas pode custar caro.

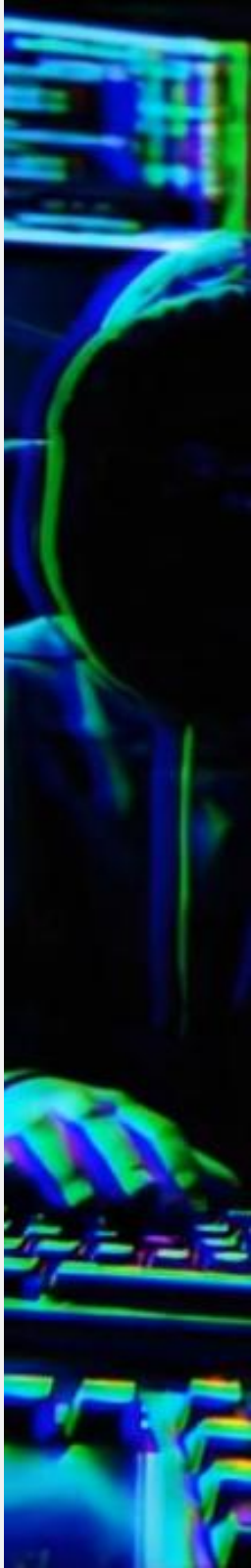
* Erro 07 Subestimar exclusões acidentais ou maliciosas

Funcionários desavisados ou mal-intencionados podem excluir dados críticos.

Após o prazo de retenção, essas informações desaparecem definitivamente.

Exemplo: em uma disputa comercial, a empresa pode ser obrigada a apresentar comunicações de anos atrás.

Sem backup independente, perde-se a capacidade de provar sua versão dos fatos.





10 Erros no backup do M365

Qualidade extrema tem método – XTR Framework

Sua organização teria hoje como recuperar e apresentar provas digitais de um contrato contestado há três anos?

* Erro 08 Não considerar o TCO real

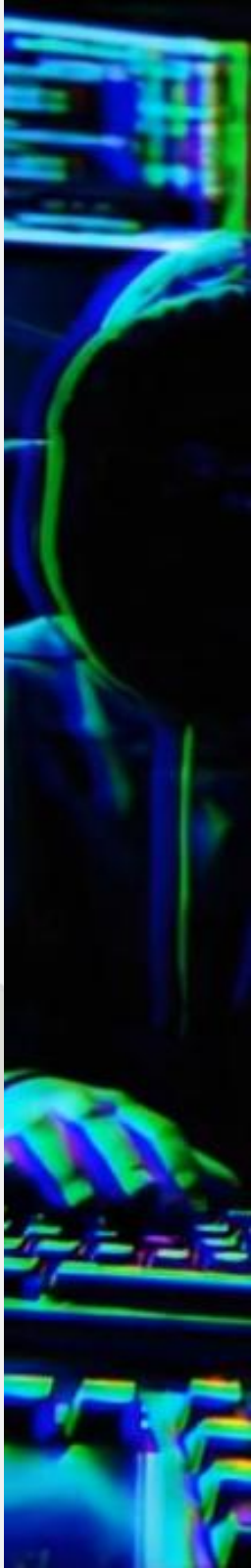
Ao avaliar backup, muitas empresas olham apenas o preço da licença.

Mas os custos ocultos, como: storage adicional, upgrades e horas de TI, elevam o TCO real, comprometendo orçamentos e desviando recursos de inovação.

Resultado: gastos crescentes, previsibilidade reduzida e dificuldade em justificar investimentos ao conselho.



O IDC aponta que até **75%** das empresas na América Latina não atingem o retorno esperado em projetos de cloud e segurança - o custo invisível da falta de governança e integração.





Grupo 03

Riscos Estratégicos

“ Quando a conta não fecha ”

* Erro 09 Ignorar o risco de ransomware em SaaS

Estar no M365 não elimina o risco de ransomware.

Ataques podem criptografar dados em OneDrive ou SharePoint, e versões corrompidas podem ser replicadas automaticamente.

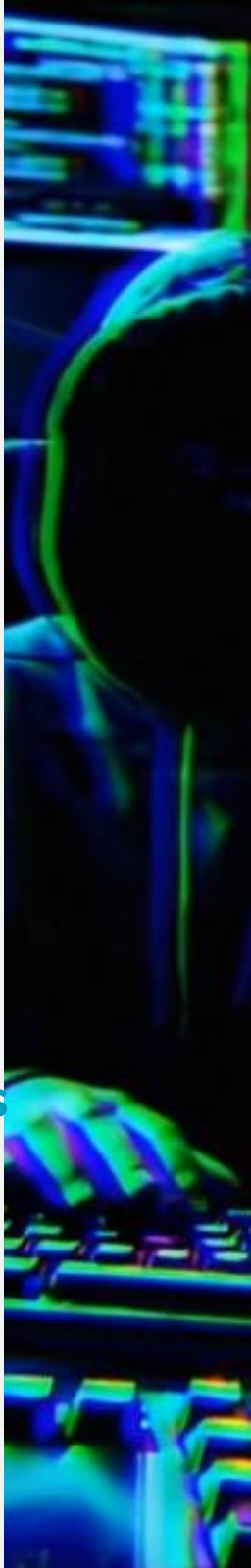
Consequência: indisponibilidade operacional e perda de confiança de clientes - mesmo com a plataforma ativa.

* Erro 10 Não contar com parceiros especializados

Depender apenas da TI interna para gerenciar backup é sobrecarregar equipes já no limite.

Sem apoio consultivo, faltam procedimentos de recuperação, testes regulares e governança estruturada.

Resultado: uma estratégia frágil, que falha justamente quando mais precisa.





10 Erros no backup do M365

Qualidade extrema tem método – XTR Framework

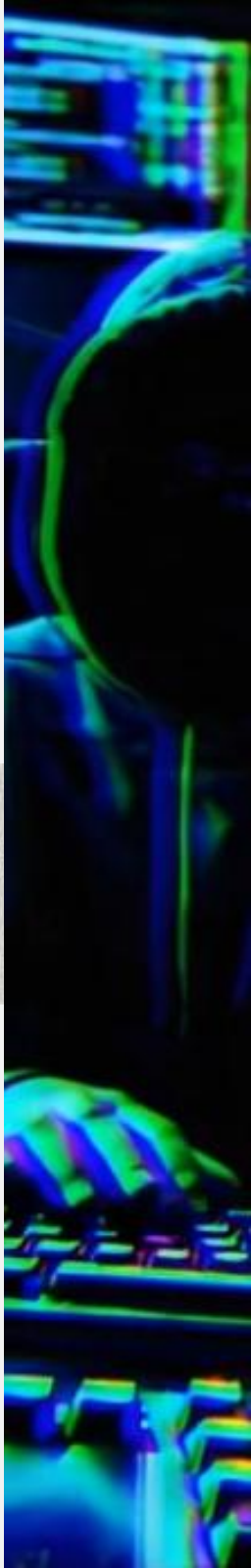
Impacto no negócio

- ROI comprometido: investimentos sem retorno tangível.
- Perda de competitividade: tempo e recursos desviados para "apagar incêndios."
- Risco jurídico: incapacidade de comprovar evidências em disputas.
- Desgaste em conselho: dificuldade em justificar custos sem resultados claros.

Não se trata apenas de perder dados - mas de perder vantagem competitiva, previsibilidade financeira e credibilidade no mercado.



**QUAL DESSES ERROS SUA
EMPRESA ESTÁ COMETENDO
HOJE?**



10 ERROS NO BACKUP DO M365

QUANDO O BACKUP FALHA



QUANDO O BACKUP FALHA: O QUE REALMENTE ACONTECE

Imagine uma empresa...

Uma multinacional do setor financeiro utiliza o Microsoft 365 como base de produtividade corporativa. Tudo parece sob controle: e-mails arquivados, documentos seguros no SharePoint, reuniões diárias no Teams.

O time de TI mantém backups regulares com uma solução tradicional e acredita estar protegido. Até que, em uma manhã comum, um ataque de phishing direcionado compromete identidades corporativas.

Em poucas horas, os dados sincronizados no OneDrive e SharePoint são criptografados e replicados automaticamente - a sincronização nativa faz o restante do estrago.

A operação para.

E, como em todo incidente real, o relógio começa a correr – contra o negócio.





O que aconteceu?

A equipe de TI reage rápido, tentando restaurar o ambiente com as ferramentas disponíveis.

Mas logo percebe que o ataque não se limitou aos usuários: as credenciais administrativas também foram comprometidas, e o tenant do M365 precisou ser colocado em quarentena pela própria Microsoft.

O que parecia uma ação de recuperação simples se transforma em um impasse:

- O backup está no mesmo domínio de confiança do ataque.
- A infraestrutura de autenticação (Entra ID) foi comprometida.
- A janela de retenção nativa não cobre todos os arquivos.
- E as tentativas de restore exigem autenticação dentro do ambiente inativo.

Resultado: o backup existe - mas não há onde restaurar.

O dado está "protegido", mas o negócio está parado.

Por que o backup falhou (mesmo existindo)

1. Falta de isolamento:

As cópias estavam armazenadas no mesmo ecossistema comprometido. Sem isolamento lógico e sem imutabilidade real, o backup se torna parte do problema, não da solução.

2. Dependência da infraestrutura afetada:

A restauração dependia do próprio ambiente de produção — servidores, identidades e permissões que agora estão sob investigação. Em um ataque de ransomware, cada dependência é um atraso.

3. Ausência de plano de retomada:

Não havia runbooks de recuperação, nem simulações prévias.

A equipe precisou reagir em tempo real, sob pressão, enquanto conselhos e auditores pediam respostas.

O impacto para o negócio:

- Financeiro: horas ou dias de inatividade, milhões em perdas indiretas e contratos adiados.
- Reputacional: clientes e investidores questionam a governança de dados da empresa.
- Regulatório: auditoria emergencial revela falhas de retenção e ausência de relatórios auditáveis.

O mais crítico: a plataforma estava disponível, mas os dados, inacessíveis. O backup existia, mas não cumpriu o papel de garantir continuidade.

O aprendido:

Esse caso não é exceção - é sintoma de uma fragilidade estrutural: a falsa sensação de segurança que o backup tradicional oferece. A verdade é que:

- O backup protege o dado, mas não o negócio.
- Ferramentas nativas ou legadas garantem cópias, mas não garantem isolamento.
- E, em um ataque real, o tempo para restaurar é maior que o tempo para perder tudo.

Para o CIO significa repensar a relação entre continuidade e infraestrutura. Para o CISO, significa reconhecer que resiliência não é uma função da TI, faz parte do negócio. A lição é clara:

Ter backup não é o bastante. O que protege a organização é a capacidade de restaurar, auditar e reagir - mesmo quando o ambiente principal está comprometido.

O ponto da virada

Esse caso ilustra o novo desafio da era SaaS:

a dependência das plataformas aumenta mais rápido do que a maturidade das estratégias de proteção.

Evitar esse cenário exige mais do que ferramentas - exige modelo, governança e preparo. É sobre isso que falaremos a seguir.

**“ O backup existia.
O negócio parou. ”**



**RESILIÊNCIA NÃO TER CÓPIAS.
É TER UM CAMINHO DE
VOLTA.**

10 ERROS NO BACKUP DO M365

IMPACTOS TÉCNICOS E EXECUTIVOS



IMPACTOS TÉCNICOS E EXECUTIVOS DOS ERROS

Dois olhares sobre o mesmo problema

As falhas de backup do Microsoft 365 não afetam apenas a operação de TI. Cada erro traz duas camadas de impacto:

- Uma técnica, visível no dia a dia da equipe.
- E outra executiva, percebida nas instâncias de decisão, auditoria e governança.

O problema é que, muitas vezes, a camada técnica é tratada - mas a executiva é ignorada. E é justamente nessa segunda camada que os danos se multiplicam.

Como diz o especialista em aviação Lito Sousa, um acidente aéreo geralmente resulta de uma sequência de erros, em que os "elos da corrente" vão se fechando. O mesmo princípio se aplica à resiliência cibernética.

Exemplos práticos

1. Exclusões não cobertas pelo backup nativo:

- Impacto técnico: usuários sem acesso a e-mails e arquivos críticos; retrabalho manual e perda de tempo operacional.
- Impacto executivo: falha em apresentar evidências em auditorias, risco jurídico e perda de credibilidade com reguladores.

A exclusão de um arquivo pode parecer um incidente simples - até virar um problema jurídico de milhões.



2. Restore lento ou incompleto:

- Impacto técnico: horas (ou dias) de indisponibilidade para equipes que dependem dos dados.
- Impacto executivo: interrupção de processos críticos - financeiro, contratos, atendimento - resultando em perda direta de receita e confiança.

O tempo técnico do restore raramente coincide com o tempo de tolerância do negócio.

3. Relatórios inconsistentes:

- Impacto técnico: sobrecarga da TI com tarefas manuais e dificuldade de consolidar informações.
- Impacto executivo: exposição a multas e sanções por não conseguir comprovar conformidade regulatória.

O que é atraso em planilha para o técnico, é falha de governança para o conselho.

4. Dependência de infraestrutura legada:

- Impacto técnico: aumento da complexidade, múltiplas interfaces e necessidade constante de upgrades.
- Impacto executivo: TCO elevado, previsibilidade financeira comprometida e dificuldade de justificar ROI em segurança e continuidade.

Cada servidor extra pesa no orçamento e fragiliza a estratégia de longo prazo.

- Para as equipes técnicas, esses erros se traduzem em sobrecarga, lentidão e retrabalho.
- Para os executivos, representam riscos de compliance, perdas financeiras e desgaste perante conselhos, clientes e reguladores.

O ponto-chave é simples, mas essencial:

Cada falha técnica é, em última instância, um risco de negócio. A maturidade vem quando o board entende que resiliência não é um investimento em TI - é um investimento em continuidade.

Conclusão e transição

Os impactos de uma falha de backup vão muito além da restauração de dados. Eles afetam a reputação, a previsibilidade financeira e a confiança - três ativos que sustentam qualquer empresa moderna.

Evitar esses erros exige uma abordagem que una tecnologia, processo e governança. E é exatamente isso que exploraremos no próximo capítulo: como transformar backup em resiliência.

Camada Técnica	Camada Executiva
Falha de exclusão	Risco jurídico e auditoria
Restore lento	Perda de receita e confiança
Relatórios inconsistentes	Falha de governança
Infraestrutura legada	TCO elevado e ROI comprometido

10 ERROS NO BACKUP DO M365

TÉCNICAS DE RESILIÊNCIA CIBERNÉTICA



Técnicas de resiliência cibernética

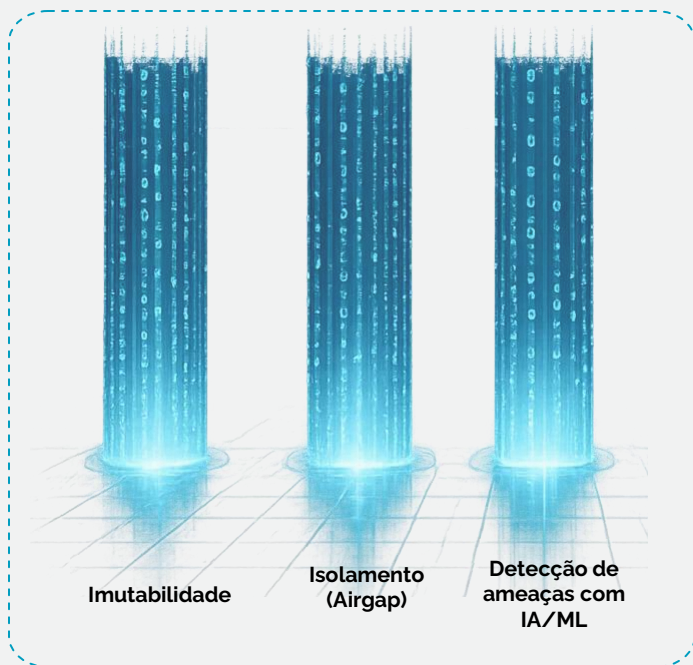
O próximo passo: do backup à resiliência

Evitar erros é apenas o primeiro movimento.

O verdadeiro diferencial está em construir uma estratégia consistente de resiliência de dados, que vá além de simplesmente “ter cópias de dados” e se alinhe a objetivos de negócio, segurança e compliance.

Empresas mais maduras já entenderam: backup é parte da equação, mas a resiliência é inegociável.

E para alcançá-la, é preciso combinar três técnicas fundamentais com governança e preparo humano.



GOVERNANÇA



Técnica 1 - Imutabilidade

A imutabilidade estabelece que existe uma versão do dado que não pode ser alterada, independentemente de quem controla o ambiente.

Isso significa: sem sobrescrita, sem alteração de metadados, sem expurgo, sem redução de retenção, mesmo que o invasor possua credenciais privilegiadas.

Não é configuração de permissão. Não é "somente leitura". Não é "trava lógica". Imutabilidade acontece abaixo do plano de controle tradicional, no nível de armazenamento ou serviço, onde não há API ou usuário capaz de alterar o estado registrado.

Ela garante que exista uma verdade inviolável, contra a qual todo ambiente pode ser reconstruído.

Mecanismo	Função	Observação
WORM (Write Once, Read Many)	Gravação não reversível a nível de storage	Deve ser enforced no hardware/firmware, não apenas em software
Retenção bloqueada (Retention Lock)	(Retention Lock)Garante retenções não editáveis, mesmo para administradores	Requer auditoria e cadeia de confiança
Versionamento Imutável	Mantém histórico íntegro de estados	Fundamental para recuperação pré-ataque
Proteção de Metadados e Catálogos	Evita corrupção de índices	Sem catálogo íntegro não existe restauração granular

Técnica 2 - Isolamento (Airgap)

Mesmo dados imutáveis se tornam inúteis se o atacante puder torná-los inacessíveis. O isolamento não é firewall, não é VLAN, não é segmentação de rede. O isolamento verdadeiro significa que o repositório resiliente não participa da superfície de ataque.

Ele opera fora do domínio de produção: não depende de Active Directory, não compartilha credenciais, não possui rotas diretas, não responde a comandos externos e não é alcançável por movimentação lateral.

No modelo de AirGap, o ambiente de cópias estratégicas funciona como um cofre de dados. Ele permanece desconectado da produção, sendo conectado apenas durante a janela controlada de transferência dos backups.

Terminado backup ou a replicação, a comunicação é bloqueada novamente. Isso significa que, mesmo que o atacante comprometa todo o ambiente produtivo, o cofre permanece fora de alcance.

Não há acesso contínuo. Não há sessão persistente. Não há canal aberto para exploração. O cofre existe para garantir que, se tudo falhar, ainda exista um ponto de reconstrução.

Isolamento é a propriedade que assegura que, mesmo sob comprometimento sistêmico, permanece um lugar onde o atacante não chegou.

E enquanto existir um lugar onde o atacante não chegou, existe caminho de volta.

Técnica 3 - Detecção de ameaças com IA/ML

Recuperar a partir de um ponto comprometido é restaurar a contaminação. Por isso, a detecção precisa ocorrer dentro do próprio ciclo de proteção, e não apenas no endpoint, no SOC ou no perímetro.

O ambiente de backup também é um espaço de observação de ataque, porque é nele que as alterações se tornam mais visíveis.

A análise precisa considerar entropia, taxa de desduplicação, variação volumétrica, comportamento anômalo de versionamento e atividade de identidades privilegiadas sobre o pipeline de proteção.

É nesse fluxo que o ransomware revela sua presença, não no momento do impacto, mas na preparação do ataque. Quando um ator malicioso compromete um ambiente, ele raramente executa a criptografia imediatamente. Ele avança em silêncio. Ele testa credenciais. Ele altera volumes gradualmente. Ele trabalha para invalidar o mecanismo de recuperação antes de interromper o ambiente.

A detecção antecipada identifica essa alteração progressiva antes da ruptura, permitindo localizar a última versão íntegra, a **Golden Copy**, que pode ser restaurada com segurança.

Sem essa validação, a restauração deixa de ser uma estratégia e passa a ser roleta russa com o negócio.

A verdadeira recuperação começa com a certeza de que se está restaurando algo íntegro.

Mas, e a governança?

Imutabilidade pode ser desativada. Isolamento pode ser relaxado. Modelos de detecção podem ser ignorados. Sem governança, tudo volta ao padrão cultural anterior: improviso, exceções, atalhos.

Governança é o que garante coerência, disciplina, permanência e auditabilidade. Ela transforma arquitetura em estado contínuo, não em projeto.

Governança não apenas documenta como operar. Ela mantém o que é inegociável. E resiliência é, sobretudo, um conjunto de métodos inegociáveis.

Resiliência é o equilíbrio entre proteção, governança e resposta. É o ponto em que tecnologia, gestão e estratégia se encontram e o negócio continua, mesmo sob ataque.



**A RESILIÊNCIA COMEÇA
ANTES DO INCIDENTE.
E CONTINUA DEPOIS
DELE.**

Boas práticas:

- Testes regulares de recuperação de workloads críticos.
- Simulações de incidentes reais (exclusões em massa, ransomware, corrupção de dados).
- Restores granulares e rápidos, compatíveis com o plano de continuidade do negócio.

Dado de referência: até 85% dos primeiros testes de restore falham em algum aspecto de execução - um alerta sobre a importância de testar antes do incidente real.

Para CIOs e CISOs, esses pilares significam transformar o backup em um ativo estratégico de continuidade:

- Menos risco regulatório, com relatórios auditáveis e automação de compliance.
- Menos impacto financeiro, com respostas rápidas e controladas.
- Mais previsibilidade de custos, com modelos SaaS escaláveis e sem CAPEX oculto.

Resiliência é o equilíbrio entre proteção, governança e resposta. É o ponto em que tecnologia, gestão e estratégia se encontram, e o negócio continua, mesmo sob ataque.



**A RESILIÊNCIA COMEÇA
ANTES DO INCIDENTE.
E CONTINUA DEPOIS
DELE.**

10 ERROS NO BACKUP DO M365

XTREME IT & DRUVA



XTREME IT & DRUVA

De BaaS a DPaaS: o salto de maturidade

Durante muito tempo, o backup foi tratado apenas como uma atividade técnica operacional. Necessária, porém isolada do restante da estratégia de continuidade.

Esse modelo resolve parte do problema, mas não garante governança, disponibilidade nem restauração confiável em caso de crise. Hoje, sem tecnologia não há negócio. Com o avanço dos ataques cibernéticos e da complexidade dos ambientes híbridos, o mercado vem amadurecendo.

Cada vez mais os boards entendem que resiliência não significa ter cópias de segurança, mas sim a capacidade de retomar a operação com confiança. E essa capacidade não surge de ferramentas isoladas, nem de equipes improvisadas. Ela exige especialização contínua, método e monitoramento permanente.

Proteção de dados e resiliência cibernética nem sempre fazem parte do core business das organizações. É nesse contexto que surge o DPaaS (Data Protection as a Service): uma evolução do BaaS, entregue pela Xtreme IT em parceria com a Druva, unindo backup, governança e resposta a incidentes em um modelo 100% SaaS, seguro e escalável.

BaaS	DPaaS
Conduta reativa	Estratégico: Antecipa riscos
Visão Técnica	Visão holística: do técnico ao negócio
Operação complexa e cara	Reduz TCO e simplifica a operação
Ações pontuais	Melhoria contínua
Gaps ocultos na gestão do ambiente	Garante continuidade do negócio





O DPaaS amplia o conceito de proteção de dados ao integrar tecnologia com forte postura de segurança e governança operacional com monitoramento e melhoria contínua.

Resumindo, não se trata apenas de salvar cópias de dados. Trata-se de garantir continuidade, conformidade e confiança (mesmo nos piores cenários).

Druva

Desafios modernos exigem uma nova abordagem de proteção de dados:

O Druva é uma plataforma centralizada de proteção de dados, desenvolvida com uma arquitetura nativa de nuvem (AWS) e com postura de segurança avançada. Por ser uma solução 100% SaaS, elimina a necessidade de investimentos em infraestrutura para backup, replicação ou cofre de dados, simplificando operações e reduzindo custos.

Construído sob os princípios de **DevSecOps**, o Druva incorpora segurança desde o design. Possui uma combinação de técnicas avançadas de segurança de dados, ao mesmo tempo, oferece alta simplicidade operacional, permitindo que equipes de TI mantenham foco na estratégia e não na manutenção de hardware ou sistemas legados.

Essa combinação de segurança, escalabilidade e simplicidade tem acelerado a adoção da plataforma globalmente. Organizações de missão crítica, como a própria NASA, utilizam o Druva para proteger dados sensíveis e garantir continuidade operacional.



O reconhecimento também é refletido no mercado: o Druva figura como **Líder no Gartner® Magic Quadrant™** para Backup and Data Protection, além de ser Customer's Choice no Gartner® Peer Insights™, com avaliação média de 4.9 (a nota máxima é 5). Uma das mais altas entre os principais fornecedores do setor.



4.9

Gartner® Peer Insights™

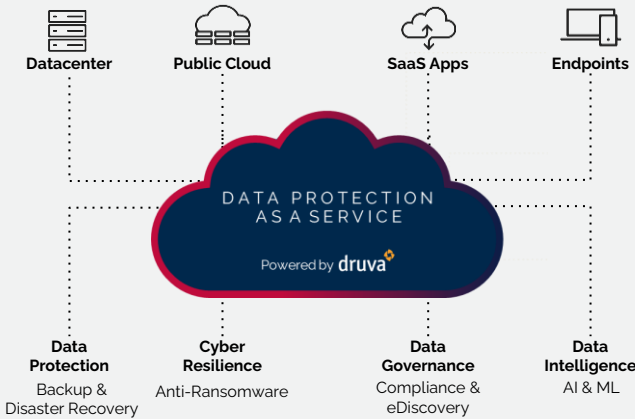
Gartner®

Magic Quadrant

Proteja qualquer workload com Druva

Com o Druva, as empresas podem proteger workloads heterogêneos num ponto centralizado de proteção:

- **Datacenter** (VMs, bancos de dados, file servers, etc).
- **Public Cloud** (Workloads nativos, kubernetes, etc).
- **SaaS Apps**: (M365, Google Workspace, Salesforce, etc).
- **Endpoints**: (Laptops e Desktops).



Principais benefícios do Druva

Com o Druva, o cliente não paga pelo egress de dados, garantindo previsibilidade financeira e permitindo restaurar os dados para qualquer ambiente.

Além disso, é possível armazenar os dados na região São Paulo (Sem custo adicional).

<p>Sem infraestrutura para gerenciar</p>	<p>Escala sob demanda</p>	<p>Deploy em minutos (Time to Value)</p>	<p>Solução 40% mais barata que as tradicionais</p>
<p>Experiência simples, porém consistente!</p>	<p>Global client-side deduplication (Incremental Forever)</p>	<p>Forte Postura de Segurança e Privacidade</p>	<p>AI & ML para detecção de ameaças</p>

Forte postura de segurança

- AI & ML para detecção de ameaças.
- Quarentena para dados suspeitos.
- Isolamento dos dados (Air-gap).
- Arquitetura 3-2-1 (Sem custo de replicação).
- Imutabilidade.
- Criptografia em transito e no repouso.
- RBAC, SSO e MFA.
- Cloud DR.
- DevSecOps.
- Remote wipe e PenTest no backup (Sem custo).
- Integração com SIEM e SOAR.
- Relatórios para auditoria.
- Recovery Scan.
- Ações de Rollback (Self-Service).
- Certificados de segurança e privacidade, como: FedRAMP, ISSO 27001, AICPA SOC3, FIPS 140-2, HIPAA, ISAE 3402, DISA, PCI e ITAR.



Druva para M365

Por que o Druva é a melhor solução para M365?

- **Exclusão acidental:** Backups automáticos diários dos dados do M365, incluindo e-mails, calendário e contatos, ajudando a proteger contra exclusões acidentais.
- **Lacunas e confusão nas políticas de retenção:** Retenção dos dados do 365 mesmo que a conta do usuário seja desativada.
- **Ameaças internas à segurança:** Mitiga o risco de perda ou destruição de dados críticos por má intenção ou incompetência.
- **Ameaças externas à segurança:** Proteção contra ameaças avançadas de e-mail, como malware e ransomware.
- **Requisitos legais e de conformidade:** O Druva vai além do backup. Com o Legal Hold, ele ajuda os usuários a localizar, preservar e reter dados que possam ser necessários para atender a solicitações legais ou investigações.





DPaaS: Quando o know-how da Xtreme IT encontra com a inovação da Druva

A importância da governança com metodologia

O que realmente faz diferença é a capacidade de continuar operando quando tudo dá errado.

Foi por isso que a Xtreme IT criou o XTR Framework, uma metodologia que estrutura, sustenta e evolui a resiliência das empresas.



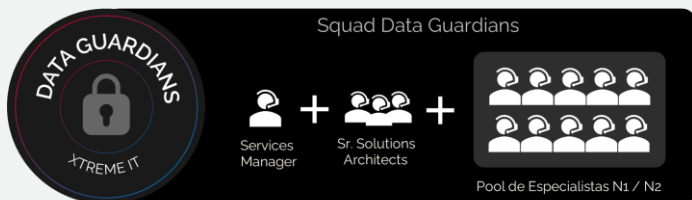
**Qualidade
extrema
tem método.**

O XTR nasceu da prática: centenas de projetos entregues, ambientes críticos protegidos e aprendizados reais sobre o que funciona (e o que não funciona) quando o jogo aperta. A metodologia usa como base os conceitos do **NIST** e **ISO27001**.

O XTR conecta tecnologia, negócio e risco. Fala a língua do board, entrega para a TI e protege o que realmente importa: a operação. Garantindo continuidade dos negócios, redução de riscos e conformidade com governança real.



Governança: XTR Framework aplicado ao DPaaS



Nosso time de especialistas compõe o Squad Data Guardians: profissionais certificados, atualizados continuamente e com forte experiência em ambientes de missão crítica.

O Squad atua na monitoração, otimização e evolução contínua do ambiente de proteção de dados, aplicando na prática os princípios do XTR Framework em cada cliente.

Está preparado para responder desde incidentes operacionais até cenários críticos, incluindo ataques de ransomware.

É esse time que sustenta a governança, disciplina e visibilidade que um serviço DPaaS exige, garantindo que o Zero Trust seja mais do que um conceito: seja a base de resiliência e continuidade para o negócio dos nossos clientes..

O próximo capítulo apresentará mais detalhes sobre o nosso Squad.

Enquanto a Druva garante a resiliência tecnológica, a Xtreme IT garante a resiliência operacional. O equilíbrio entre segurança, eficiência e conformidade.



Entregamos além da tecnologia

Com a parceria Xtreme IT & Druva, as organizações evoluem de uma visão limitada (BaaS) para um modelo integrado de proteção e continuidade (DPaaS):

- Mais que armazenar cópias, é garantir a continuidade do negócio.
- Menos sobrecarga para TI, mais foco em inovação e eficiência.
- Alinhamento direto às agendas de resiliência, compliance e otimização de custos.

O resultado é maturidade: uma proteção invisível no dia a dia, mas decisiva quando o imprevisto acontece.

A resiliência de dados não se mede apenas por RTO e RPO, mas pela capacidade de o negócio continuar funcionando, mesmo sob pressão. Com a abordagem Xtreme IT + Druva, entregamos:

- **Redução de TCO:** custos previsíveis, sem investimentos em hardware, IaaS ou manutenção.
- **Agilidade operacional:** restores granulares em minutos, sem impacto à produtividade.
- **Conformidade garantida:** relatórios auditáveis, alinhados a padrões regulatórios.
- **Confiança executiva:** menos risco de interrupções, multas ou danos à reputação.

Cada decisão técnica é sustentada por uma visão executiva. Proteger o dado é proteger o negócio.

**“ BACKUP SALVA DADOS.
DPaaS PROTEGE REPUTAÇÕES. ”**



10 ERROS NO BACKUP DO M365

SQUAD DATA GUARDIANS



SQUAD DATA GUARDIANS

A tecnologia sozinha não basta

Backup não é apenas uma ferramenta. Sem governança, acompanhamento e pessoas qualificadas, a tecnologia se torna mais um sistema para administrar - e não uma solução para proteger o negócio.

É aqui que entra a célula de serviços da Xtreme IT.

Nosso papel é transformar a proteção de dados em um processo vivo, contínuo e alinhado à estratégia da organização.

A resiliência não se instala - ela se constrói e se mantém.

Entregamos além da tecnologia

Arquitetos e consultores formam o nosso "SQUAD DATA GUARDIANS", uma verdadeira tropa de elite técnica e muito experiente com vivência em ambientes missão-crítica. O squad atua como extensão da equipe de TI, trazendo visão técnica e executiva.

Eles ajudam a transformar o backup em uma estratégia de negócio mensurável, não apenas em uma tarefa operacional.

“ Resiliência viva é feita de método, pessoas e propósito. ”

Governança e compliance na prática

Resiliência exige disciplina. Por isso, nossas rotinas são estruturadas em processos claros e auditáveis, que sustentam a conformidade e a transparência.

- Criação e manutenção de runbooks de recuperação.
- Relatórios executivos e técnicos prontos para auditorias.
- Ajuste contínuo das políticas conforme mudanças regulatórias ou de negócio.

Governança não é sobre controle. É sobre confiança.

Resposta a incidentes

Quando um incidente ocorre, tempo e coordenação são tudo.

Nossa equipe atua lado a lado com o cliente, conduzindo ações de resposta, mitigação e aprendizado.

- Apoio em simulações e testes de recuperação.
- Acompanhamento durante crises reais, reduzindo impacto e acelerando retomada.
- Orientação consultiva para evitar recorrências e fortalecer processos.

Em momentos críticos, o que faz diferença não é a ferramenta - é quem está ao seu lado.

Evolução contínua

Resiliência é movimento. Por isso, mantemos um ciclo constante de aprimoramento, baseado em evidências e boas práticas globais.

- Avaliações trimestrais do ambiente.
- Recomendações de eficiência e alinhamento estratégico.
- Atualização constante das práticas de segurança e recuperação.

A cada ciclo, o ambiente fica mais preparado, eficiente e previsível.

Enquanto a Druva oferece a confiabilidade global da tecnologia SaaS, a Xtreme IT assegura que essa tecnologia seja aplicada de forma prática, contextualizada e eficaz no cenário brasileiro.

Nosso diferencial é claro:

Não entregamos apenas tecnologia.

Entregamos resiliência sustentada por pessoas, processos e método.

A combinação entre expertise técnica, metodologia e acompanhamento constante cria um ecossistema em que o backup deixa de ser uma operação - e se torna um ativo estratégico de continuidade e confiança.



10 ERROS NO BACKUP DO M365

CAMINHO PRÁTICO DE ADOÇÃO





CAMINHO PRÁTICO DE ADOÇÃO

Simplicidade com método

Transformar backup em resiliência pode parecer complexo. Mas a experiência da Xtreme IT mostra que, com método e clareza, o caminho é rápido, previsível e sem ruptura.

Nosso processo é estruturado para gerar valor desde o primeiro passo, equilibrando eficiência técnica e alinhamento estratégico.

A jornada acontece em quatro etapas complementares, que transformam intenção em resultado real:

1. Diagnóstico Executivo (30 minutos)

Tudo começa com uma conversa estruturada entre CIO, CISO e equipe técnica. O objetivo é mapear lacunas de proteção de dados, identificar riscos e alinhar as prioridades de negócio.

Resultado: uma visão clara do nível atual de maturidade e das oportunidades de evolução imediata.

2. Prova de Conceito (POC)

Em um ambiente controlado do Microsoft 365, é feita a implantação prática da solução, sem impacto para o ambiente produtivo. A equipe do cliente participa ativamente, validando a performance, a governança e a experiência de uso.

Resultado: validação prática da abordagem e confiança na aplicabilidade da solução.

3. Rollout com Governança

Com a prova de conceito validada, inicia-se a expansão estruturada da proteção de dados. Cada fase é acompanhada pela equipe Xtreme IT, garantindo:

- Políticas de retenção alinhadas às exigências regulatórias;
- Relatórios executivos e técnicos configurados;
- Integrações com outros sistemas corporativos.

Resultado: ambiente protegido, auditável e totalmente aderente às políticas de compliance.

4. Avaliações Contínuas

Resiliência não é um projeto, é um processo.

Por isso, realizamos avaliações trimestrais para revisar métricas, ajustar políticas e incorporar novas práticas de segurança e governança. Cada ciclo gera relatórios executivos com recomendações de aprimoramento, conectando tecnologia e estratégia.

Resultado: resiliência como processo vivo, em evolução constante frente a novos riscos e regulações.

Essa jornada foi desenhada para que a resiliência comece simples e se torne natural.

Sem burocracia, sem sobrecarga e com foco total em resultado mensurável. Para o CIO e o CISO, isso significa:

- Clareza sobre riscos e prioridades.
- Validação técnica antes da decisão.
- Implementação assistida e governança comprovada.
- Melhoria contínua sem interrupções.

A resiliência não é um projeto de TI - é uma jornada de evolução do negócio. E o primeiro passo pode começar em uma simples conversa de 30 minutos.





Resiliência não é destino. É jornada.

O novo imperativo dos negócios

A proteção de dados deixou de ser uma função técnica.

Hoje, ela é um pilar estratégico da continuidade e da confiança - um elo entre tecnologia, governança e reputação.

CIOs e CISOs não são mais apenas guardiões de sistemas: são protetores da confiança digital que sustenta clientes, investidores e o próprio valor da marca.

E a confiança não se improvisa — ela se constrói com método, visibilidade e resposta rápida.

Do backup à resiliência

O cenário atual exige mais do que armazenar cópias de segurança. Exige orquestrar proteção, governança e resposta, de forma integrada, testada e mensurável. É aqui que o modelo DPaaS (Data Protection as a Service) redefine o jogo:

- Simplicidade operacional, sem infraestrutura adicional.
- Automação e compliance contínuos, com relatórios auditáveis.
- Suporte especializado, que transforma tecnologia em resultado.

Junto à Druva, a Xtreme IT traduz esse conceito em realidade, combinando uma plataforma global de classe mundial com um time local de especialistas, que entende as particularidades do mercado brasileiro e das exigências regulatórias da região.

O papel da liderança

A verdadeira transformação começa com uma decisão de liderança: mudar a forma de pensar sobre proteção de dados.

Não se trata de "ter um backup", mas de garantir a continuidade operacional mesmo diante do inesperado.

Empresas que tratam a resiliência como diferencial competitivo colhem:

- Menos risco.
- Mais eficiência.
- Maior confiança dos clientes e do mercado.

Um convite à ação

Se sua organização reconhece que o Microsoft 365 é o coração da produtividade, é hora de garantir que ele também seja o núcleo da resiliência.

O primeiro passo pode ser simples — uma conversa de 30 minutos com nossa equipe para entender o nível atual de maturidade do seu ambiente e identificar caminhos práticos para evoluir.

Fale com nossos especialistas e descubra como transformar backup em resiliência viva. Com método, tecnologia e pessoas certas ao seu lado.

“ Resiliência é capacidade de antecipar, reagir e evoluir. ”

10 ERROS NO BACKUP DO M365

OBRIGADO!



REFERÊNCIAS BIBLIOGRÁFICAS

Microsoft Shared Responsibility Model:

Fonte: <https://learn.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility>

Microsoft Digital Defense Report 2024 (Threat Landscape Overview):

Fonte: <https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report>

CrowdStrike Global Threat Report 2025:

Fonte: <https://www.crowdstrike.com/pt-br/global-threat-report/>

Dell Global Data Protection Index 2024:

Fonte: <https://www.dell.com/en-us/lp/data-protection-gdpi>

IDC MarketScape (Latin America Public Cloud Infrastructure as a Service):

Fonte: <https://my.idc.com/getdoc.jsp?containerId=LA50933123&pageType=PRINTFRIENDLY>

IDC Showcases (IDC Data Protection Survey):

Fonte: <https://www.idc.com/custom-solutions/custom-showcase/>

Fonte: https://www.cristie.com/wp-content/uploads/2024/09/IDC-White-Paper_State-of-DR-and-Cyber-Recovery-2025-2025_US52445524.pdf



CRÉDITOS

Desenvolvido e escrito por:

- Ciro Missola – Xtreme IT
- Ivan Felipe – Xtreme IT

Produzido por:

- Rodrigo Teixeira – Octogen

Agradecimentos:

Agradecemos a todos os profissionais da Xtreme IT e a Druva, que contribuíram direta ou indiretamente para a criação deste material. Em especial, aos clientes que nos inspiram diariamente a elevar o padrão de proteção e resiliência dos ambientes corporativos no Brasil.

Resiliência não se constrói sozinho, ela nasce da colaboração, da confiança e do propósito compartilhado

15
ANOS

XTREME IT



CYBERSECURITY
AWARENESS
MONTH