RELATÓRIO

O Estado do Ransomware na Educação 2026

Resultados de uma pesquisa independente com 226 líderes de TI e segurança cibernética do setor de educação distribuídos em 17 países e cujas organizações foram atingidas por ransomware no último ano.

SOPHOS

Introdução

Bem-vindo à sexta edição do relatório anual da Sophos sobre o Estado do Ransomware na Educação, que revela a realidade do ransomware para instituições de ensino fundamental e médio (incluindo escolas de ensino básico, fundamental e médio — geralmente para alunos menores de 18 anos) e de ensino superior (universidades, faculdades e estabelecimentos equivalentes — geralmente para alunos maiores de 18 anos) em 2026.

O relatório deste ano também lança nova luz sobre áreas anteriormente inexploradas, incluindo onde os ataques começam no ambiente, o papel defensivo da autenticação multifator (MFA) e dos firewalls, e a conexão entre ataques de identidade e ransomware.

Com base nas experiências reais de 226 líderes de TI e cibersegurança na área da educação, sendo 131 de instituições de ensino fundamental e 95 de ensino superior, que foram atingidos por ransomware no último ano, este relatório oferece informações exclusivas sobre:

- Métodos de ataque e defesa
- Criptografia e recuperação de dados
- Pedidos de resgate e pagamentos
- Impacto nos negócios e nas pessoas

Nota: Ao longo deste relatório, "pesquisa geral" refere-se aos resultados dos entrevistados em todos os setores pesquisados. Os 226 entrevistados do setor da educação fazem parte de um grupo maior de 2.158 respondentes em 15 setores da indústria.

Sobre a pesquisa

Este relatório baseia-se nas conclusões de um levantamento independente e totalmente desvinculado de fornecedores encomendado pela Sophos. A pesquisa incluiu perguntas sobre experiências organizacionais com ataques de ransomware e invasões baseadas em identidade, rastreando índices de pagamento de resgate, custos de recuperação, tempo de recuperação e outras métricas ano a ano. As respostas foram coletadas de janeiro a março de 2026 e baseiam-se nas experiências dos entrevistados nos 12 meses anteriores.

Os participantes vieram de 17 países e 15 setores econômicos, abrangendo uma ampla gama de indústrias nos setores público e privado, e representaram uma curva de amostragem de empresas com tamanhos entre 100 e 5 mil funcionários, que se manteve proporcionalmente consistente ao longo dos seis anos de duração da pesquisa. Todos os dados financeiros são expressos em dólares americanos.

Principais descobertas

- **Os ataques de identidade, especialmente os baseados em e-mail, apresentaram índices elevados nos setores da educação.**
  - 77% das vítimas do ensino superior e 71% das do ensino básico confirmaram que o ataque de ransomware que sofreram também foi o ataque de identidade mais significativo, ambos acima dos 67% registrados na pesquisa geral (todos os setores).
  - E-mails maliciosos foram a principal causa técnica de ataques de ransomware no ensino básico (31%) e no ensino superior (29%).
  - Abordagens baseadas em identidade (por exemplo, e-mails maliciosos, phishing, credenciais comprometidas ou força bruta) foram responsáveis por 85% dos ataques em instituições de ensino, superando os 79% da pesquisa geral (todos os setores).
- **As fragilidades operacionais no setor da educação foram superiores às apontadas na pesquisa geral (todos os setores).**
  - A principal lacuna no ensino superior foi a expertise: 53% afirmaram não possuir as habilidades necessárias para detectar e impedir o ataque a tempo, em comparação com 35% na pesquisa geral.
  - As principais causas operacionais do ensino básico foram erro humano (52%), falta de proteção (47%), lacunas de segurança desconhecidas (42%) e falta de pessoal ou capacidade (41%).
- **A incidência de criptografia decorrente dos ataques de ransomware aumentou drasticamente no ensino básico.**
  - A taxa de criptografia de dados no ensino básico mais que dobrou, passando de 29% em 2025 para 61% em 2026.
  - 58% dos ataques ao setor educacional resultaram em dados criptografados, um índice próximo aos 56% da pesquisa geral.
- **As instituições de ensino do setor da educação dependeram fortemente de backups para restaurar os dados.**
  - 77% das instituições de ensino básico restauraram dados criptografados a partir de backups, superando a taxa de 66% registrada na pesquisa geral.
  - 69% das instituições de ensino superior também se recuperaram utilizando backups.
- **O setor da educação pagou menos do que a pesquisa geral, mas registrou mais pagamentos de resgate acima de US$ 5 milhões.**
  - O valor mediano exigido para resgates no setor da educação foi superior ao da pesquisa geral, atingindo US$ 775,2 mil (contra US$ 698 mil), mas o valor mediano pago em resgates foi menor, de US$ 515 mil (contra US$ 769 mil no geral).
  - A mediana dos pedidos de resgate setor da educação diminuíram por dois anos consecutivos, enquanto os pagamentos aumentaram em US$ 15 mil entre o relatório de 2025 e o de 2026.
  - As instituições do setor da educação foram mais propensas a pagar US$ 5 milhões ou mais (23% contra 16% na pesquisa geral).
- **A recuperação no setor da educação custou mais e levou mais tempo.**
  - Os custos médios de recuperação na educação atingiram US$ 2,26 milhões, valor superior a US$ 1,7 milhão na pesquisa geral.
  - Os custos de recuperação do ensino aumentaram desde o relatório de 2025, passando de US$ 1,66 milhão para US$ 2,26 milhões, com os custos do ensino superior aumentando em mais de US$ 1 milhão.
  - 26% das instituições de ensino precisaram de um a três meses para se recuperar totalmente de um ataque de ransomware, quase o dobro da taxa de 14% observada em todos os setores.
  - O ensino básico foi o que apresentou a maior parcela de recuperações de longo prazo: 31% levaram um mês ou mais para se recuperar, mais do que qualquer outro setor.
- **O impacto humano sobre as equipes de segurança intensificou-se.**
  - 53% das equipes do ensino superior relataram aumento da pressão por parte da alta administração, em comparação com 40% entre todos os setores.
  - Aproximadamente 39% das equipes de ensino relataram ausência de funcionários devido a estresse ou problemas de saúde mental, em comparação com 29% em todos os setores.

Métodos de ataque e defesa

Causas primárias dos ataques

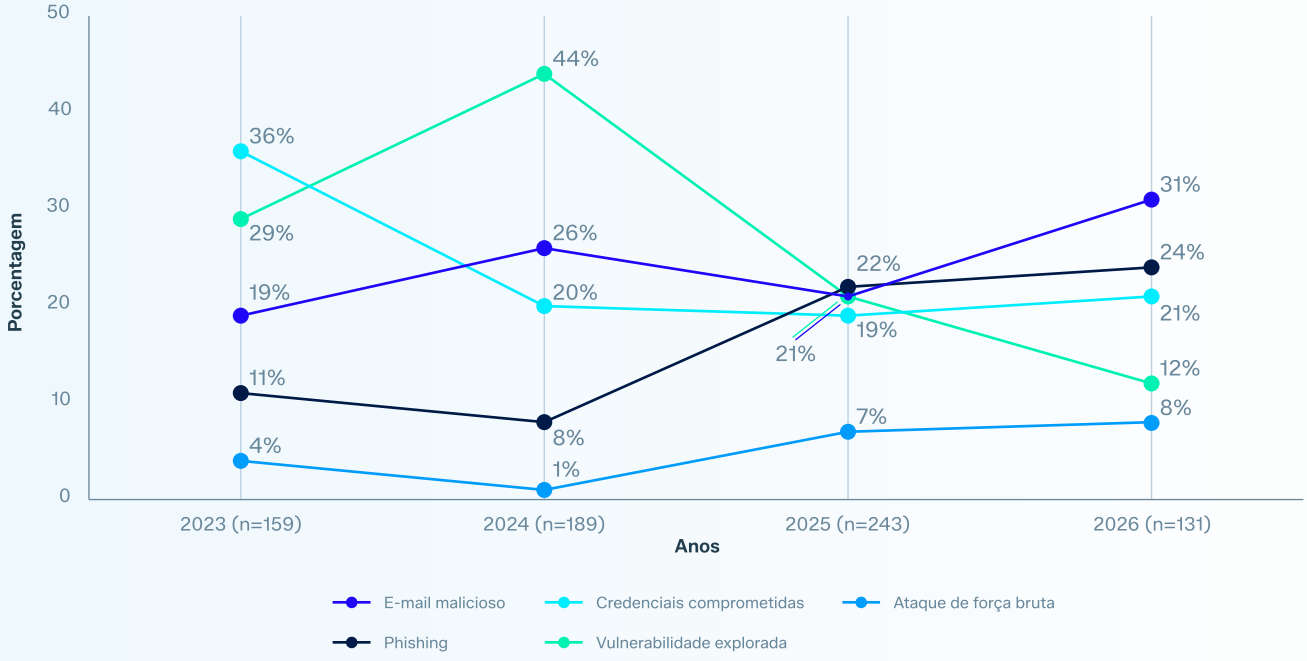
Os dados do setor da educação deste ano refletem a mesma mudança observada em todos os setores: os ataques baseados em identidade estão aumentando.

E-mails maliciosos foram a causa técnica primária mais comum no ensino básico (31%), seguidos por phishing (24%) e credenciais comprometidas (21%). As vulnerabilidades exploradas caíram para 12%, o que reflete a queda geral na pesquisa geral (todos os setores) para 18%.

85%

A proporção de ataques a provedores de ensino que começaram com uma abordagem baseada em identidade (por exemplo, e-mail malicioso, phishing, credenciais comprometidas ou força bruta) ficou acima da taxa geral da pesquisa, que foi de 79%.

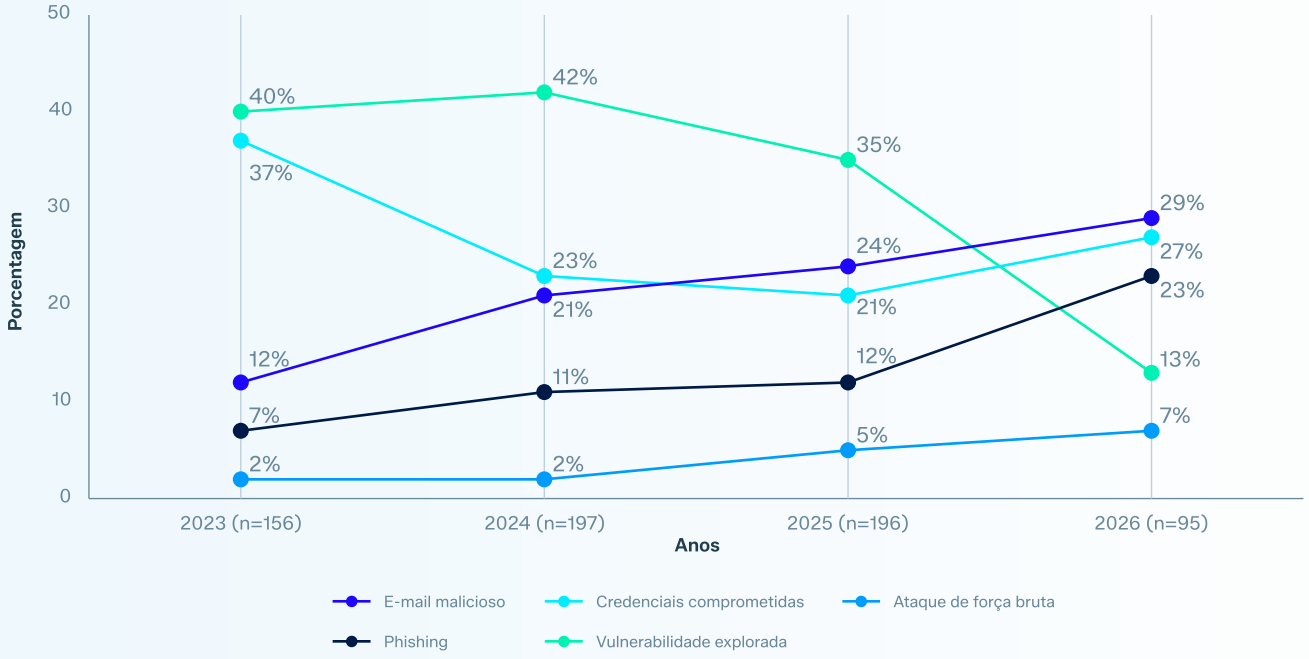
Causa técnica primária dos ataques de ransomware 2023–2026: Ensino fundamental



Você sabe a causa primária do ataque de ransomware que a sua organização enfrentou no último ano?
Download e "Não sei" removidos do gráfico para clareza visual. As porcentagens podem não totalizar 100%. Números de base no gráfico.

As instituições de ensino superior também relataram uma queda nas vulnerabilidades exploradas. Esse vetor caiu para 13% no relatório de 2026, ante 35% em 2025. **E-mails maliciosos (29%) e credenciais comprometidas (27%) são as principais causas, com o phishing (23%) logo atrás** Tanto o ensino básico quanto o superior relatam ataques via e-mail como as principais causas, o que está em consonância com a pesquisa geral, na qual e-mails maliciosos (26%) e phishing (24%) juntos representam metade de todos os incidentes.

Causa técnica primária dos ataques de ransomware 2023–2026: Ensino superior

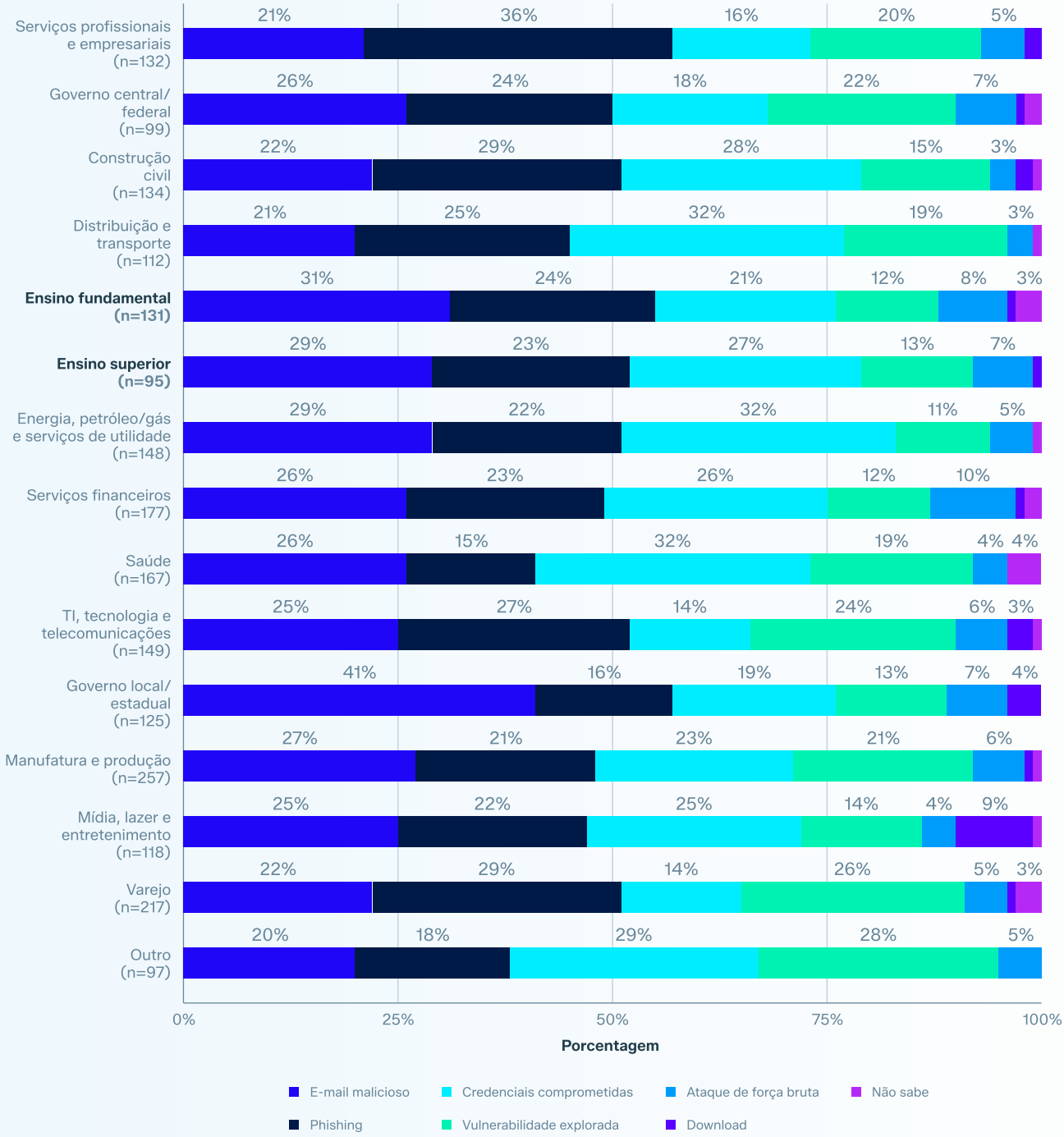


Você sabe a causa primária do ataque de ransomware que a sua organização enfrentou no último ano?
Download e "Não sei" removidos do gráfico para clareza visual. As porcentagens podem não totalizar 100%. Números de base no gráfico.

Em conjunto, **vetores baseados em identidade (por exemplo, e-mails maliciosos, phishing, credenciais comprometidas e ataques de força bruta) representaram 85% dos ataques a instituições de ensino, acima dos 79% registrados na pesquisa geral**. O ensino superior apresentou a maior proporção, com 86%, seguido pelo ensino básico, com 84%. Em outras palavras, aproximadamente seis em cada sete ataques contra instituições de ensino começaram com uma abordagem baseada em identidade, reforçando a importância da segurança da identidade para a defesa do setor.

O setor da educação reflete uma mudança intersetorial mais ampla: aumento dos ataques realizados por e-mail e redução dos relatos de vulnerabilidades exploradas. No entanto,os especialistas da Sophos preveem que as explorações de vulnerabilidades voltem a aumentar, visto que as organizações têm dificuldades para acompanhar o ritmo dos patches de correção de vulnerabilidades identificadas pela IA fronteiriça.

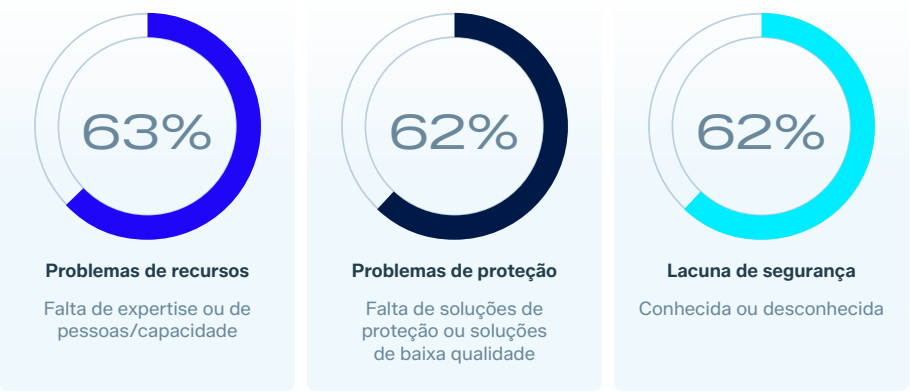
Causa técnica primária por setor (2026)



Você sabe a causa primária do ataque de ransomware que a sua organização enfrentou no último ano? Números de base no gráfico.

O que deixou as organizações vulneráveis

As instituições de ensino citaram uma ampla gama de problemas de proteção, recursos e lacunas de segurança. Nas três categorias consolidadas, os problemas de recursos (falta de pessoal ou de competências) foram citados por 63% dos prestadores de serviços de educação, seguidos por problemas de proteção (62%) e lacunas de segurança (62%).



Por que você acha que a sua organização foi vítima de um ataque de ransomware? n=226. Respostas consolidadas.

A educação combinada apresentou uma taxa mais alta do que a pesquisa geral em quase todas as causas operacionais primárias, com as lacunas de segurança conhecidas sendo a única exceção. A separação entre educação básica e ensino superior revela duas fragilidades distintas.

A principal fragilidade do ensino superior foi a falta de expertise. 53% afirmaram não possuir as habilidades ou o conhecimento necessários para detectar e impedir o ataque a tempo, em comparação com 35% na pesquisa geral, uma diferença de 18 pontos percentuais, a maior já registrada.

As fragilidades da educação básica concentravam-se em torno da capacidade e das ferramentas. O erro humano foi citado por 52% dos prestadores de serviços de educação básica (contra 35% em todos os setores), a falta de proteção por 47% dos prestadores e a falta de pessoal ou capacidade por 41% dos prestadores.

53%

A proporção de vítimas do ensino superior que afirmaram não possuir as habilidades ou o conhecimento necessários para detectar e impedir o ataque a tempo, 18 pontos percentuais acima da média da pesquisa, representa sua maior fragilidade.

Causas operacionais primárias: ensino fundamental e superior comparado a todos os setores

Causa operacional primária	Ensino fundamental (n=131)	Ensino superior (n=95)	Todos os setores (n=2.158)
Falta de proteção	47%	36%	36%
Lacuna de segurança desconhecida	42%	38%	36%
Lacuna de segurança conhecida	33%	35%	36%
Falta de pessoas/ capacidade	41%	37%	35%
Erro humano	52%	36%	35%
Falta de expertise	33%	53%	35%
Baixa qualidade de proteção	38%	39%	33%

Por que você acha que a sua organização foi vítima de um ataque de ransomware? São permitidas múltiplas respostas. Números de base no gráfico.

Em comparação com outros setores, o setor de educação enfrentava dificuldades devido à falta de proteção e de expertise. A tabela abaixo mostra os setores distribuídos na coluna da causa operacional primária mais citada.

Principal causa operacional primária dos ataques de ransomware por setor

FALTA DE PROTEÇÃO	LACUNA DE SEGURANÇA DESCONHE-CIDA	LACUNA DE SEGURANÇA CONHECIDA	FALTA DE PESSOAS/ CAPACIDADE	FALTA DE EXPERTISE	BAIXA QUALIDADE DE PROTEÇÃO	ERRO HUMANO
Não tínhamos os produtos e serviços de segurança cibernética necessários em operação	Havia um ponto fraco em nossas defesas do qual não tínhamos conhecimento	Tínhamos pontos fracos em nossas defesas dos quais estávamos cientes, mas que não havíamos abordado.	Não tínhamos um número suficiente de especialistas em segurança cibernética monitorando nossos sistemas no momento do ataque.	Não tínhamos as habilidades ou conhecimento à disposição para detectar e interromper o ataque em tempo hábil	Nossos produtos e serviços de segurança cibernética não foram capazes de interromper o ataque	Nossas equipes cometeram um erro/não seguiram os processos corretamente.
Serviços profissionais e empresariais (44%)	TI, tecnologia e telecomuni-cações (42%)	Serviços financeiros (44%)	Mídia, lazer e entretenimento (43%)	**Ensino superior (53%)**	Distribuição e transporte (38%)	**Ensino fundamental (52%)**
Outros (42%)	Construção civil (41%)	Varejo (38%)	Governo local/ estadual (42%)	Saúde (47%)		Manufatura e produção (39%)
Energia, petróleo/ gás e serviços de utilidade (37%)		Energia, petróleo/ gás e serviços de utilidade (37%)		Governo central/ federal (43%)		

Por que você acha que a sua organização foi vítima de um ataque de ransomware? São permitidas múltiplas respostas. Os setores ligados por múltiplas causas estão marcados com um asterisco (*). n=2.158.

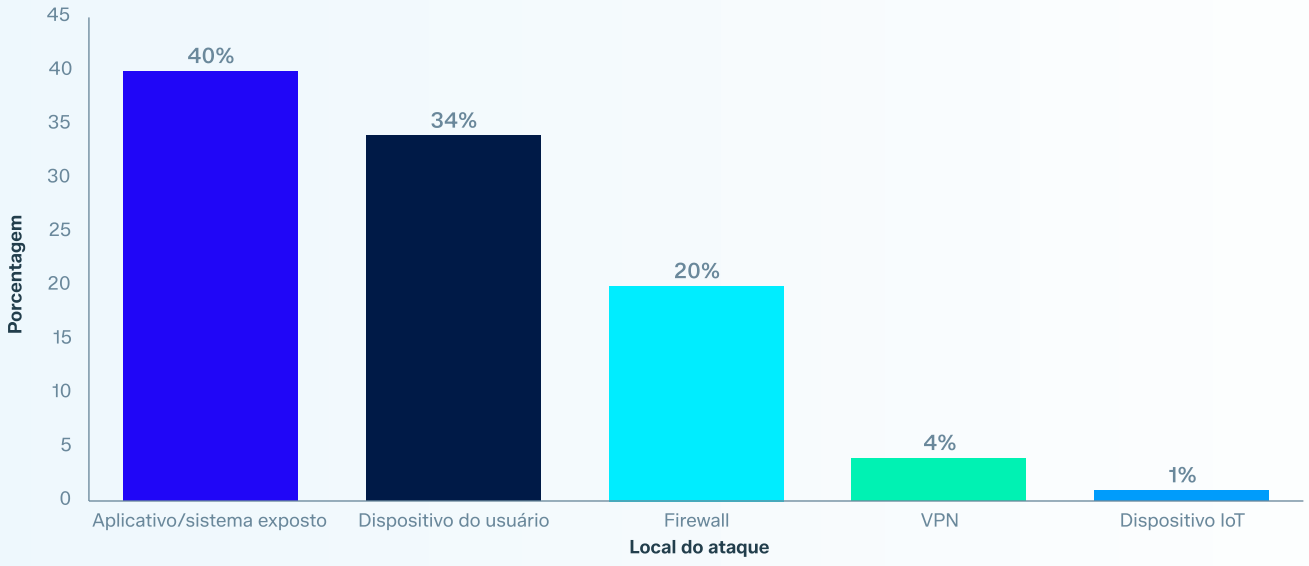
NOVA PESQUISA

Onde começam os ataques

Uma nova pesquisa deste ano levanta a questão de onde, no ambiente, os ataques começaram, especificamente entre os incidentes que tiveram início com uma vulnerabilidade explorada, credenciais comprometidas ou um ataque de força bruta.

Na educação, os aplicativos e sistemas expostos foram o ponto de entrada mais comum (40%), seguidos por dispositivos de usuário (34%) e firewalls (20%). Esses números acompanham de perto a pesquisa geral (38%, 30% e 21%, respectivamente), portanto, a educação não apresenta divergência significativa nesse aspecto.

Onde começam os ataques de ransomware: Educação combinada



Você disse que a causa raiz foi uma vulnerabilidade explorada, credenciais comprometidas ou um ataque de força bruta. Em que parte do seu ambiente isso aconteceu? Ensino superior e básico combinados. n=99

NOVA PESQUISA

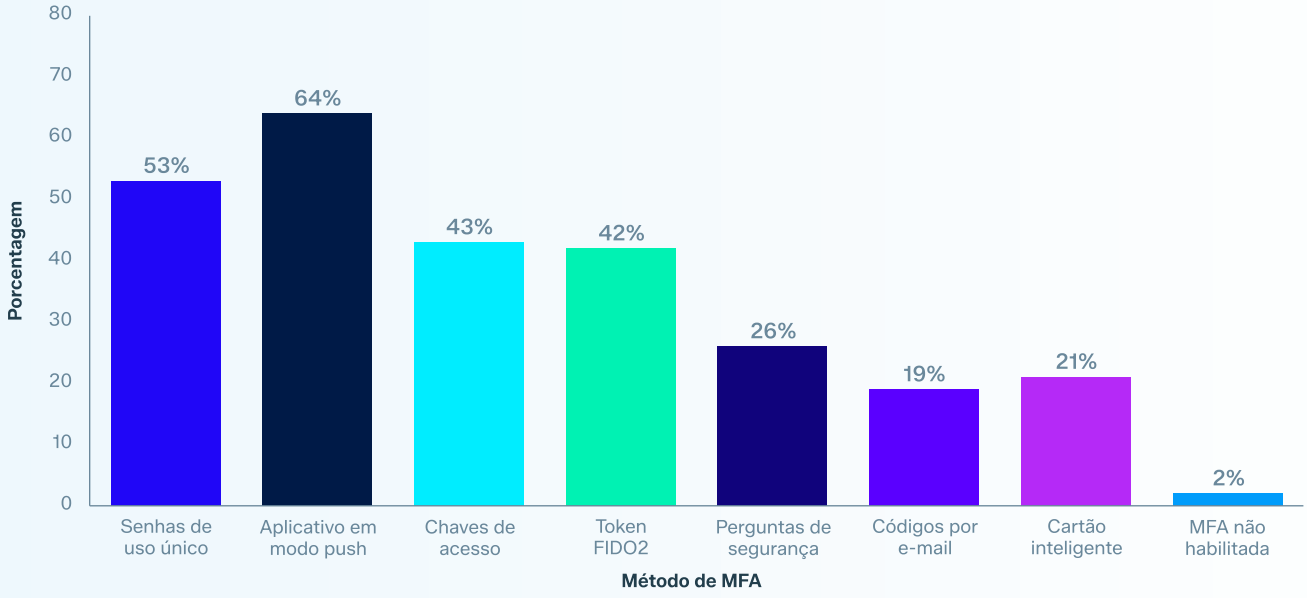
O papel da autenticação multifator (MFA)

Também examinamos os métodos de autenticação multifator (MFA) em vigor no momento do ataque entre os provedores de educação cujo ataque começou com credenciais comprometidas. Quase todas as vítimas na área da educação tinham alguma forma de autenticação multifator (MFA) habilitada (98%), o que corrobora a conclusão geral da pesquisa (97%) de que a MFA estava presente na maioria dos ataques baseados em credenciais.

No entanto, entre os provedores de educação que foram questionados sobre a autenticação multifator (MFA), 81% ainda mantinham os dados criptografados, apesar da ativação da MFA. Isso sugere que ou a autenticação multifator (MFA) não foi implementada de forma abrangente em todos os sistemas críticos, ou os invasores encontraram maneiras de contornar as proteções da MFA, ou ainda os vetores de ataque não se basearam exclusivamente em credenciais comprometidas.

Aplicativos baseados em notificações push (64%) e senhas de uso único (53%) foram os métodos mais comumente implementados no setor educacional.

Métodos de MFA habilitados no momento do ataque: Educação combinada



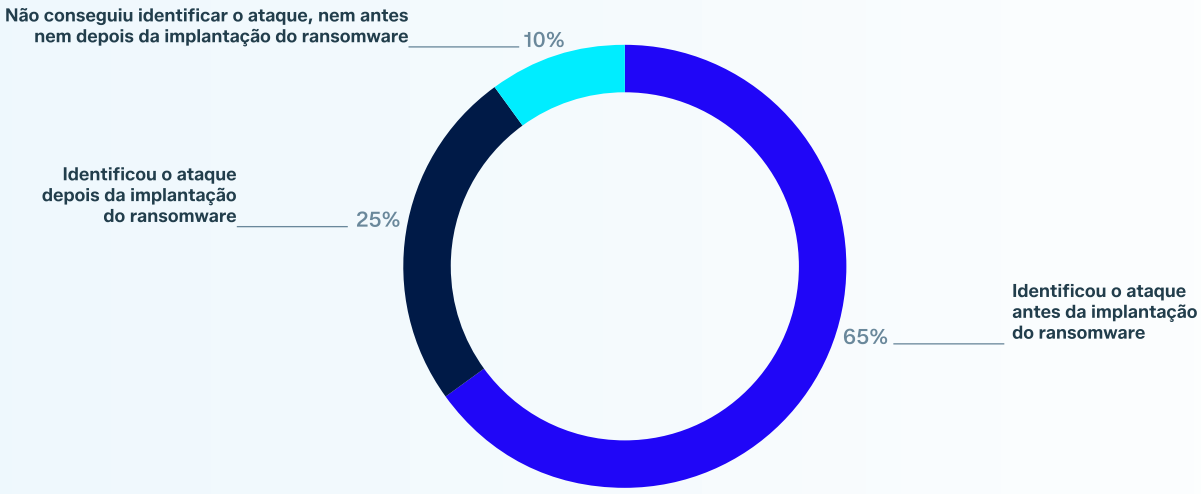
Que tipo de autenticação multifator estava habilitada no momento do ataque, se alguma? São permitidas múltiplas respostas.
Base: O ataque ocorreu devido a credenciais comprometidas. Ensino superior e básico combinados. n=53.

NOVA PESQUISA

O papel dos firewalls

Na área da educação, os firewalls identificavam a maioria dos ataques, mas nem sempre ajudavam a impedi-los. 65% dos provedores afirmaram que seu firewall identificou o ataque antes da implantação do ransomware, 25% disseram que o identificou posteriormente e 10% disseram que não identificou o ataque de forma alguma. Isso reflete a pesquisa geral (61%, 32% e 7%), com uma ligeira mudança em direção às duas extremidades do espectro.

Qual foi o papel do seu firewall na identificação do ataque?



Qual foi o papel do seu firewall na identificação do ataque? Ensino superior e básico combinados. n=226.

Entre os casos de detecção precoce, as vítimas do setor da educação ainda tinham seus dados criptografados em 51% dos casos.

Os firewalls estão fazendo um bom trabalho na coleta de dados para identificar ataques, mas os ataques ainda não estão sendo bloqueados na mesma proporção em que são identificados. Os firewalls geralmente registram os dados necessários para detectar e interromper um ataque, mas podem não estar suficientemente integrados a outros sistemas para reconhecer a ameaça e responder a tempo.

NOVA PESQUISA

A relação entre identidade e ransomware

Uma das conclusões mais claras da pesquisa é a ligação direta entre ataques de identidade e ransomware. Em todos os setores, dois terços das vítimas de ransomware (67%) confirmaram que o incidente foi o mesmo que o ataque de identidade mais significativo que sofreram. No entanto, a educação está acima dessa marca: 71% no ensino fundamental e 77% no ensino superior (73% em educação combinada).

Embora nem todos os ataques tenham resultado em criptografia de dados, a descoberta mostra uma forte sobreposição entre ataques de identidade e ransomware na área da educação.

O ataque de ransomware também foi o ataque mais significativo relacionado à identidade

Sua organização sofreu um ataque de ransomware que também foi um ataque de identidade? Organizações atingidas por ransomware. Bases nos gráficos.

73%

A proporção de vítimas no setor educacional cujo incidente de ransomware coincidiu com o ataque de identidade mais significativo que sofreram, acima da taxa geral da pesquisa, que é de 67%.

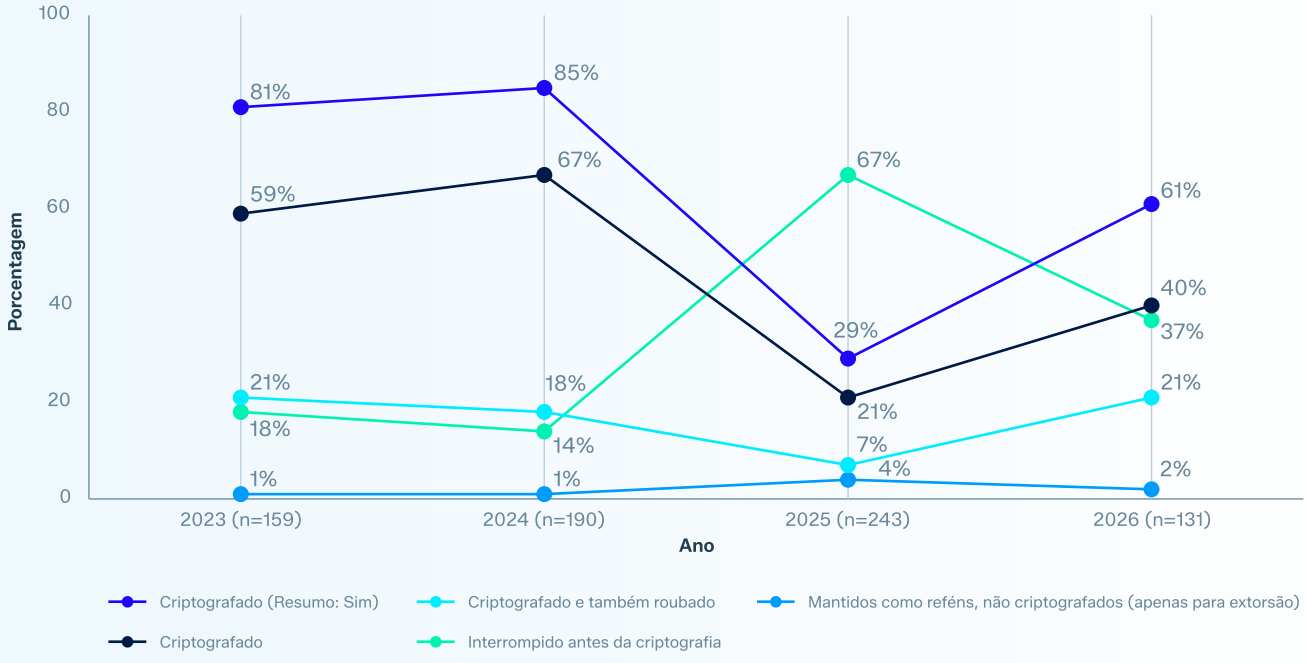
Criptografia e recuperação de dados

Taxa de criptografia de dados

Os resultados do Relatório sobre o Estado do Ransomware na Educação em 2025 mostraram impactos muito positivos no ensino fundamental. Infelizmente, o relatório deste ano mostra que o ensino fundamental está regredindo, aproximando-se da tendência anterior.

Após a taxa de criptografia de dados no ensino fundamental ter caído para 29% no relatório de 2025, a mais baixa de qualquer setor naquele ano, **a proporção de ataques contra o ensino fundamental que conseguiram criptografar dados mais que dobrou, chegando a 61% em 2026.** (acima da taxa geral da pesquisa, que é de 56%). Apenas 37% dos ataques foram impedidos antes da criptografia pelo ensino fundamental este ano, uma queda em relação aos 67% registrados no relatório do ano passado.

Taxa de criptografia de dados ao longo do tempo: Ensino fundamental

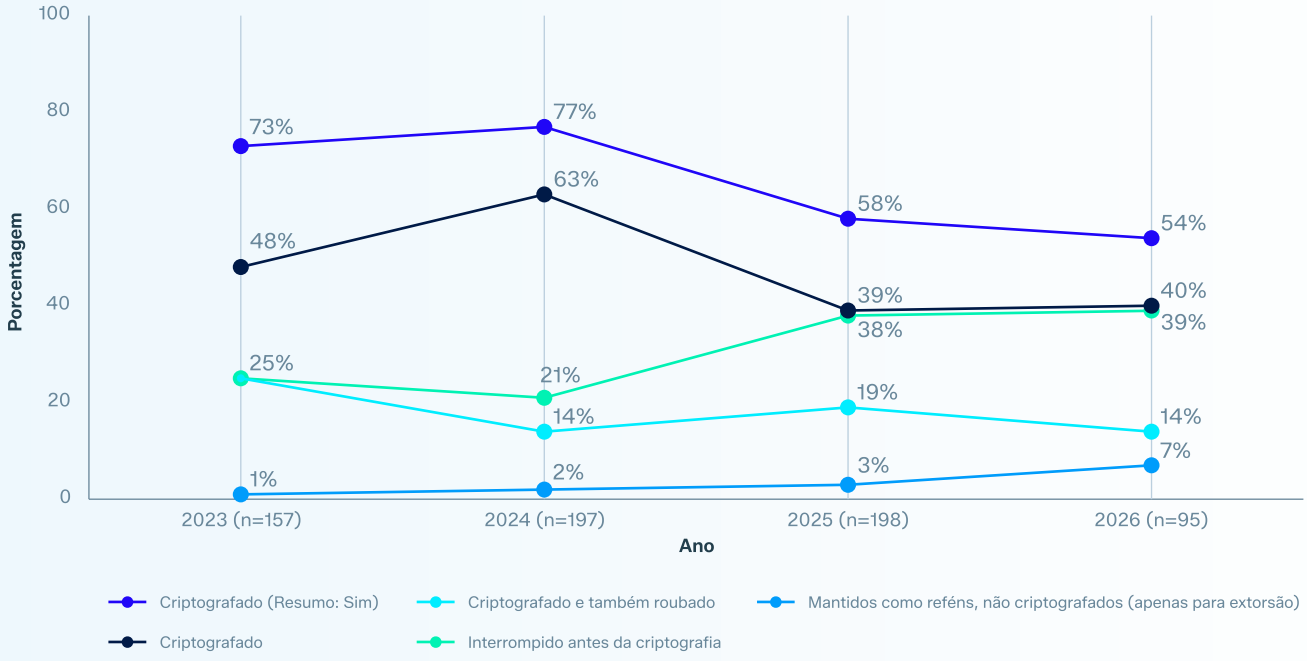


Os criminosos virtuais tiveram sucesso na criptografia de dados da sua organização no ataque de ransomware? Números de base no gráfico. A linha "Criptografado (Resumo: Sim)" neste gráfico é a soma das respostas "Criptografado" e "Criptografado e também roubado".

A dupla extorsão (em que os dados são criptografados e também roubados) ressurgiu no ensino fundamental, subindo de 7% em 2025 para 21% em 2026, alinhado aos níveis anteriores a 2025. Esses ataques oferecem aos atacantes um segundo ponto de vantagem. Os ataques de extorsão apenas**(com pedido de resgate sem criptografia)** caíram ligeiramente, de 4% para 2%, no ensino fundamental.

O ensino superior foi mais estável. Sua taxa de criptografia diminuiu ligeiramente para 54% em 2026, de 58% em 2025, mantendo-a próxima à taxa da pesquisa geral.

Taxa de criptografia de dados ao longo do tempo: Ensino superior



Os criminosos virtuais tiveram sucesso na criptografia de dados da sua organização no ataque de ransomware? Números de base no gráfico. A linha "Criptografado (Resumo: Sim)" neste gráfico é a soma das respostas "Criptografado" e "Criptografado e também roubado".

No ensino superior, os ataques de extorsão aumentaram para 7%, ante 3% em 2025, o que é digno de atenção, mesmo que represente uma pequena parcela.

O cenário de 2026 também retoma o padrão de longo prazo da educação. Em 2023 e 2024, a taxa de criptografia de dados no ensino fundamental foi maior do que no ensino superior; 2025 foi a exceção, quando a taxa no ensino fundamental caiu drasticamente por um breve período. A taxa de criptografia de 61% neste ano para o ensino fundamental, em comparação com 54% para o ensino superior, restabelece a tendência de longo prazo.

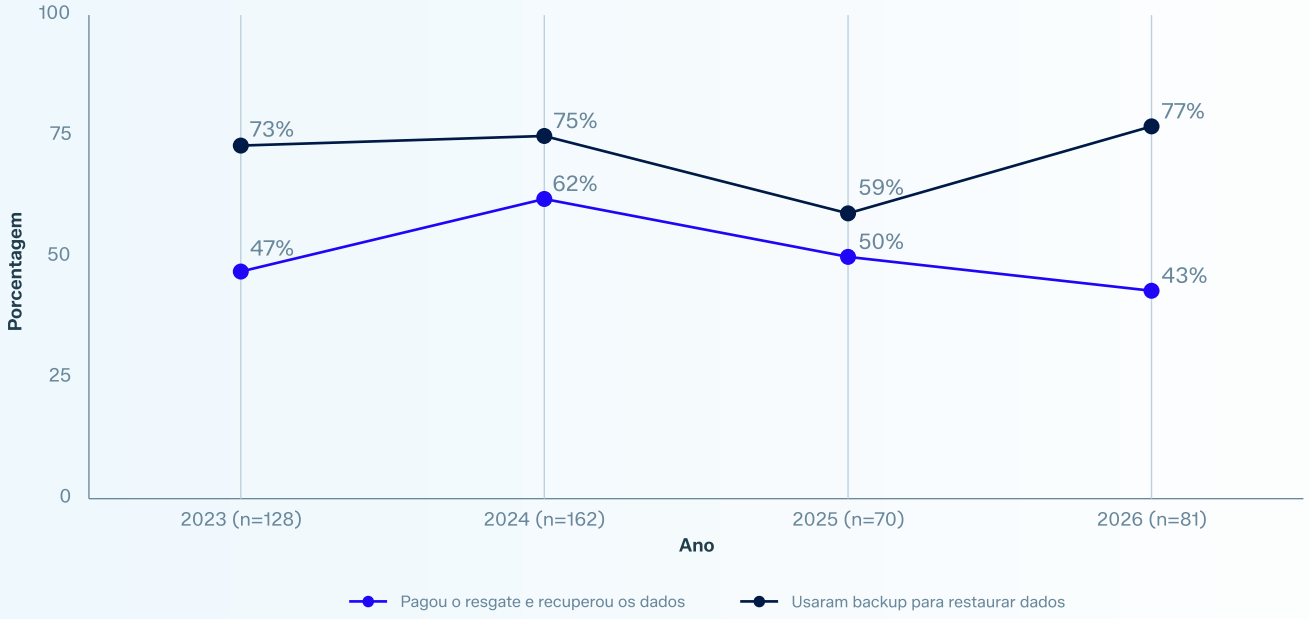
Como as organizações recuperaram dados criptografados

Em 2026, o backup foi a principal alavanca de recuperação das instituições de ensino. Após uma queda em 2025 (59% no ensino fundamental e 47% no ensino superior), a recuperação baseada em backup se reergueu este ano. **77% dos provedores de ensino básico e 69% dos provedores de ensino superior restauraram dados a partir de backups**, ambos acima da taxa da pesquisa geral de 66%. Essa reerguida sugere que as instituições de ensino renovaram seus investimentos em infraestrutura de backup e estão reconstruindo sua resiliência contra pedidos de resgate.

77%

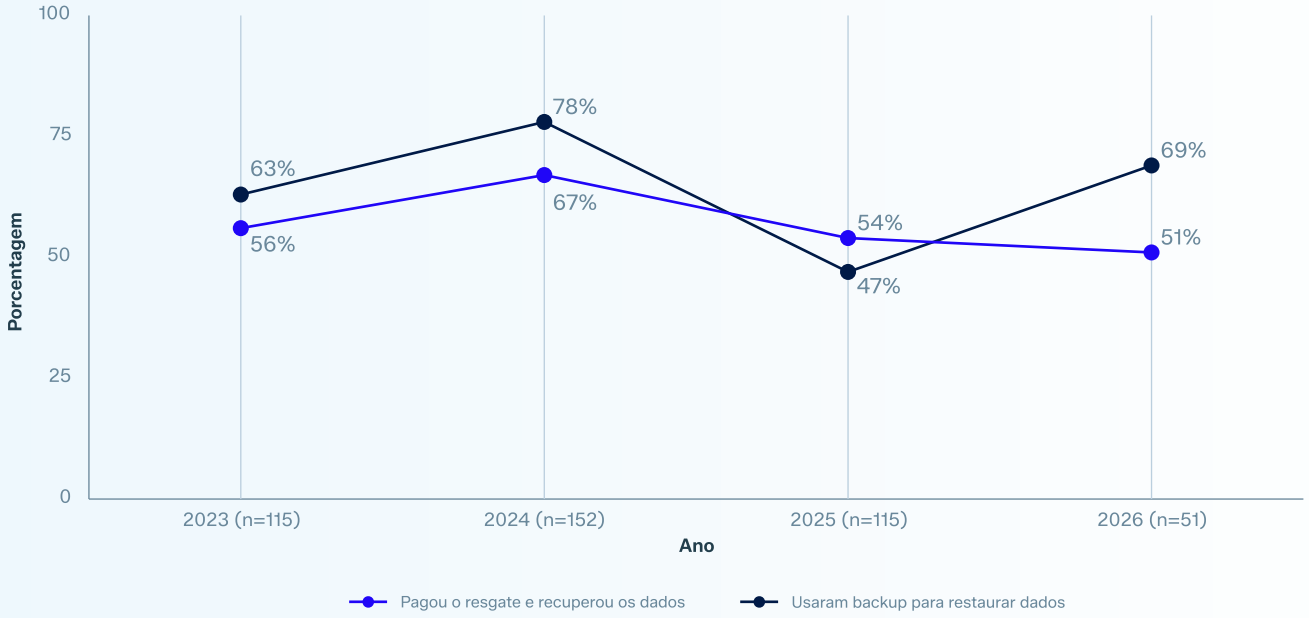
A proporção de instituições de ensino básico que restauraram dados criptografados a partir de backups em 2026 ficou acima da taxa geral da pesquisa, que foi de 66%.

Métodos de recuperação de dados ao longo do tempo: Ensino fundamental



Como sua organização recuperou os dados? São permitidas múltiplas respostas. Números de base no gráfico.

Métodos de recuperação de dados ao longo do tempo: Ensino superior



Como sua organização recuperou os dados? São permitidas múltiplas respostas. Números de base no gráfico.

Ao mesmo tempo, o setor da educação está pagando resgates com menos frequência. **A proporção de provedores que pagaram o resgate e recuperaram os dados diminuiu por dois anos consecutivos** , de 62% (2024) para 50% (2025) e para 43% (2026) no ensino fundamental, e de 67% para 54% e para 51%, respectivamente, no ensino superior.

Com o aumento da restauração de backup e a queda da recuperação baseada em pagamentos, as instituições de ensino estão se recuperando mais pela força de suas próprias capacidades do que pela cooperação dos atacantes.

Pedidos de resgate e pagamentos

Pedidos de resgate

O setor da educação enfrentou exigências de resgate mais elevadas em comparação com outros setores na pesquisa geral. O valor mediano exigido em resgates às instituições de ensino foi de US$ 775,2 mil, acima da mediana de US$ 698 mil de todos os outros setores. A distribuição também apresentou uma assimetria positiva: **metade dos pedidos de resgate (50%) foi de US$ 1 milhão ou mais, e um quarto (25%) foi de US$ 5 milhões ou mais**, em comparação com 46% e 23%, respectivamente, na amostragem de todos os setores.

Nota: Valores de resgate atípicos, iguais ou superiores a 40 milhões de dólares, foram removidos desses dados.

Valor mediano do pedido de resgate

	2025	2026
Educação	US$ 0,98 mi (n=185)	US$ 0,78 mi (n=132)
Todos os setores	US$ 1,32 mi (n=1.700)	US$ 0,70 mi (n=1,214)

Qual foi o valor do pedido de resgate exigido pelos invasores? Base: organizações cujos dados foram criptografados. Números de base no gráfico.

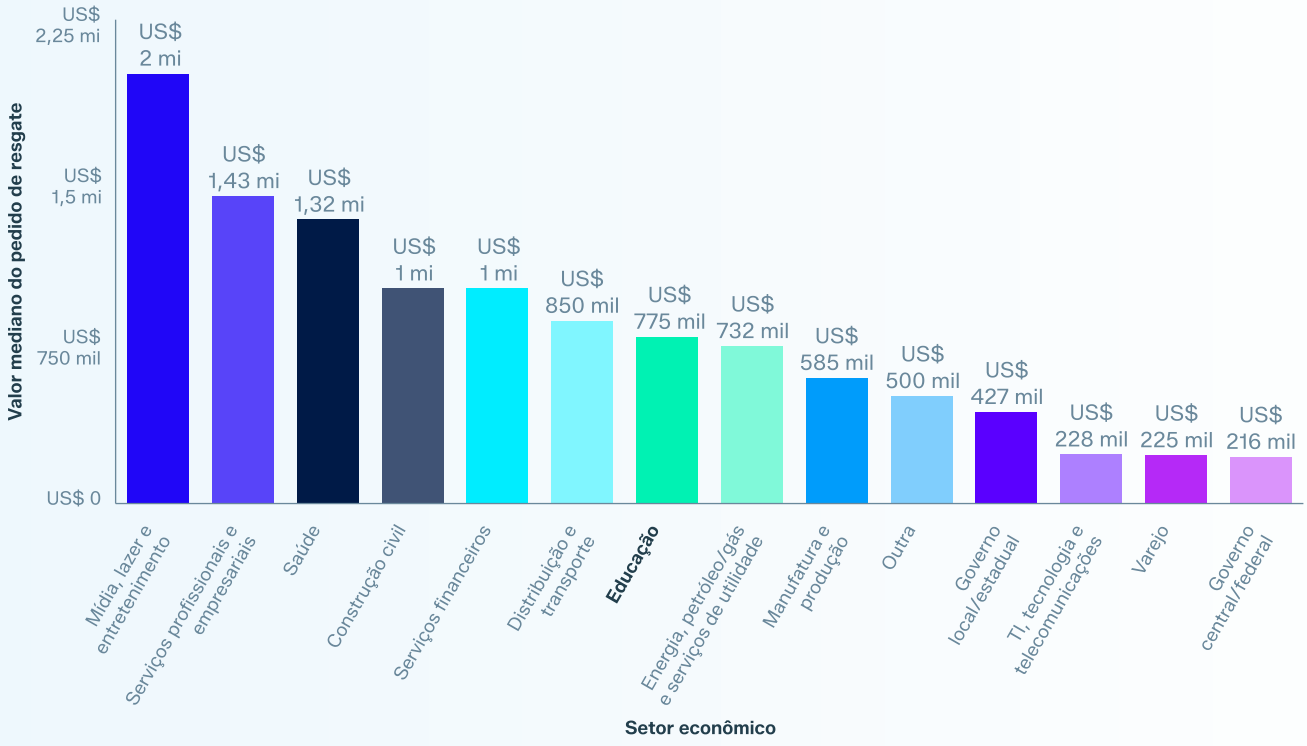
Em comparação com outros setores, a educação ocupa uma posição intermediária. Seu valor mediano de resgates exigidos fica abaixo dos setores com exigências mais altas, como mídia, lazer e entretenimento (US$ 2 milhões) e serviços profissionais e empresariais (US$ 1,43 milhão), mas bem acima de setores com exigências mais baixas, como governo central (US$ 216,5 mil) e varejo (US$ 225 mil).

US$ 775,2 mil

O valor mediano exigido em resgates às instituições de ensino — superior à mediana da pesquisa geral, de US$ 698 mil.

Metade de todos os pedidos de resgate relacionados à educação foram de US$ 1 milhão ou mais.

Mediana de pedidos de resgate por setor



Qual foi o valor do pedido de resgate exigido pelos invasores? Base: organizações cujos dados foram criptografados. n=1.141

As tendências anuais são boas e ruins. A exigência mediana de resgates na educação combinada caiu de US$ 976 mil em 2025 para US$ 775,2 mil em 2026. Essa queda foi impulsionada principalmente pelo ensino fundamental, onde a demanda mediana caiu de US$ 1,03 milhão para US$ 737,6 mil, enquanto o ensino superior apresentou uma tendência contrária, com sua demanda mediana subindo de US$ 697,086 mil para US$ 889,2 mil.

Pagamentos de resgate

Os altos resgates exigidos do setor da educação não se traduziram em pagamentos mais altos. **Embora tenham enfrentado pedidos de resgate mais elevados, a mediana de resgate pago pelo setor da educação foi menor em comparação com outros setores na pesquisa geral**. O valor mediano pago em resgates por uma instituição de ensino foi de US$ 515 mil, abaixo da mediana pesquisa geral, que foi de US$ 769 mil.

Os pagamentos do setor da educação se concentraram fora da faixa mais alta, mas incluíram uma parcela maior de pagamentos superiores a US$ 5 milhões. 39% dos pagamentos relacionados à educação foram de US$ 1 milhão ou mais, percentual inferior aos 44% da pesquisa geral. No entanto, 23% foram de US$ 5 milhões ou mais, acima da taxa da pesquisa geral de 16%. Quando a educação paga, normalmente paga valores menores do que os de outros setores, mas uma minoria significativa desembolsa quantias muito elevadas.

Mediana de pagamento de resgate

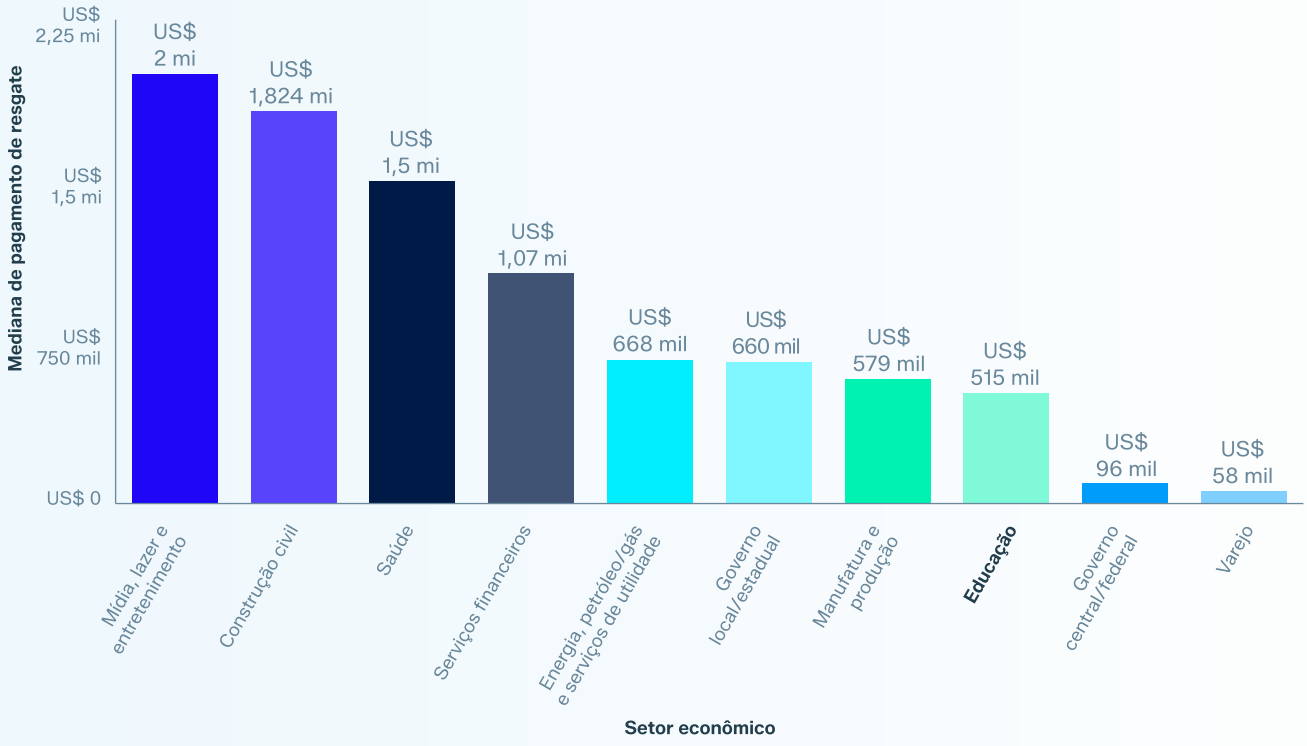
	2025	2026
Educação	US$ 0,50 mi (n=100)	US$ 0,52 mi (n=62)
Todos os setores	US$ 1 mi (n=847)	US$ 0,77 mi (n=587)

Aproximadamente qual foi o valor do resgate pago aos atacantes? Base: organizações que pagaram o resgate. Números de base no gráfico.

US$ 515 mil

O valor mediano dos resgates pagos por instituições de ensino foi inferior à mediana geral da pesquisa, de US$ 769 mil, apesar das exigências de resgate serem mais altas.

Mediana de pagamento de resgate por setor



Aproximadamente qual foi o valor do resgate pago aos atacantes? Base: organizações que pagaram o resgate. n=587. Exclui setores com menos de 30 entrevistados para esta pergunta.

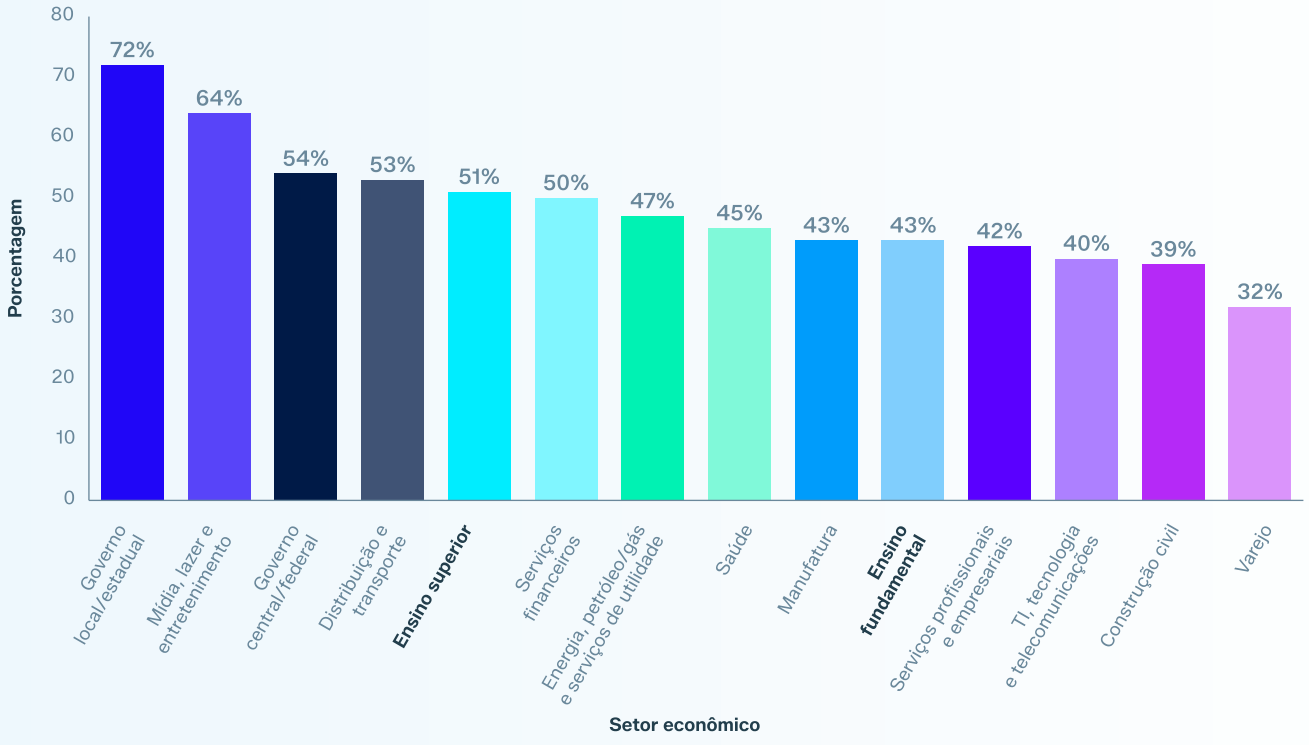
As tendências anuais também foram díspares em relação aos pagamentos de resgate. O pagamento mediano da educação combinada permaneceu essencialmente estável, com um leve aumento de US$ 500 mil em 2025 para US$ 515 mil em 2026. O pagamento mediano no ensino fundamental caiu drasticamente no mesmo período, de US$ 800 mil para US$ 320 mil. O ligeiro aumento no nível combinado foi, portanto, impulsionado pelo ensino superior.

Como menos de 30 instituições de ensino superior registraram o valor do pagamento este ano (n=27), não podemos apresentar uma tendência distinta e confiável dos pagamentos do ensino superior, portanto, recomendamos usar as tendências de pagamento da educação combinada.

Percentagem de organizações que pagaram o resgate, por setor.

A propensão a pagar resgates se mostrou diferente entre os dois segmentos da educação. 51% das vítimas do ensino superior pagaram o resgate, acima da taxa geral de 48%, enquanto 43% das vítimas do ensino fundamental pagaram o resgate, sendo mais relutantes em efetuar o pagamento do que a taxa geral.

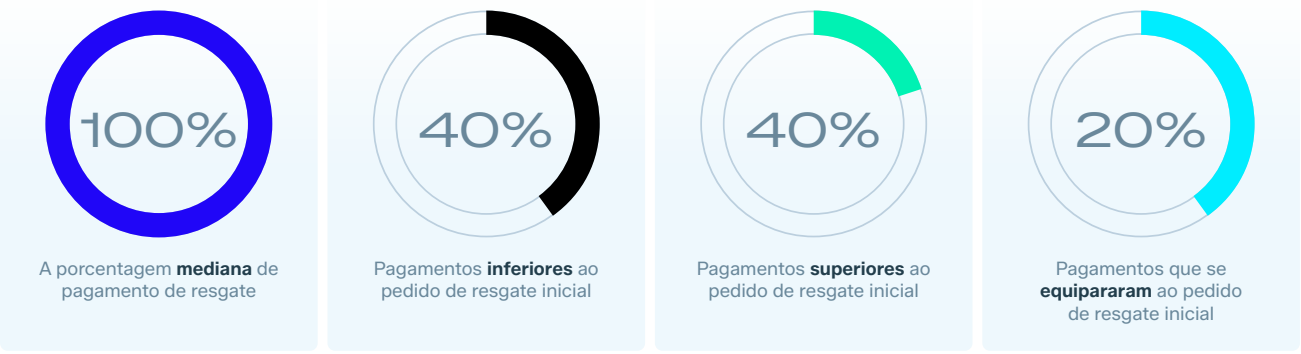
Porcentagem de quem pagou o resgate por setor



Como sua organização recuperou os dados? Base: organizações cujos dados foram criptografados. n=1.214

Pagamentos reais comparado a exigências iniciais

Entre as instituições de ensino que pagaram o resgate, 40% pagaram menos do que o valor inicialmente exigido, 40% pagaram mais e 20% pagaram exatamente o valor solicitado. A instituição mediana pagou 100% do resgate exigido, um aumento em relação aos 82% registrados em 2025. Assim, embora uma parcela substancial das instituições tenha negociado a redução do valor pago, uma parcela igual acabou pagando mais do que o inicialmente exigido.



Considerando o valor do resgate pago, ele foi menor, igual ou maior que o valor inicial exigido? Excluindo valores atípicos Ensino superior e básico combinados. n=58.

Impacto nos negócios e nas pessoas

Custos de recuperação de ransomware

O setor da educação encarou uma despesa de recuperação acima da média. **O custo médio para remediar um ataque de ransomware, excluindo qualquer resgate pago, foi de US$ 2,46 milhões no ensino fundamental e US$ 1,99 milhão no ensino superior**, ambos acima da média geral da pesquisa, de US$ 1,7 milhão.

O ensino básico suportou o fardo mais pesado por dois anos consecutivos. O custo médio de recuperação do ensino básico subiu de US$ 2,28 milhões em 2025 para US$ 2,46 milhões em 2026, fazendo dele o setor da educação mais caro e bem acima da pesquisa geral (US$ 1,7 milhão).

Custo médio de recuperação

	2025	2026
Ensino fundamental	US$ 2,28 mi (n=243)	US$ 2,46 mi (n=131)
Ensino superior	US$ 0,90 mi (n=198)	US$ 1,99 mi (n=95)
Todos os setores	US$ 1,53 mi (n=3,400)	US$ 1,70 mi (n=2,158)

Qual foi o custo aproximado para sua organização para remediar os impactos do ataque de ransomware mais significativo? Média, excluindo resgates pagos. Números de base no gráfico.

Foi no ensino superior que a lacuna se ampliou mais acentuadamente. Seu custo médio de recuperação mais que dobrou, passando de US$ 0,90 milhão em 2025 para US$ 1,99 milhão em 2026. No relatório de 2025, o ensino superior registrou um dos custos de recuperação mais baixos de todos os setores. Este ano esse custo aumentou, aproximando-se do ensino fundamental. Ambos os segmentos de educação agora estão acima da média geral da pesquisa, que, por sua vez, subiu modestamente de US$ 1,53 milhão para US$ 1,7 milhão.

US$ 1,09 mi

Aumento nos custos médios de recuperação de ataques de ransomware no ensino superior entre 2025 e 2026.

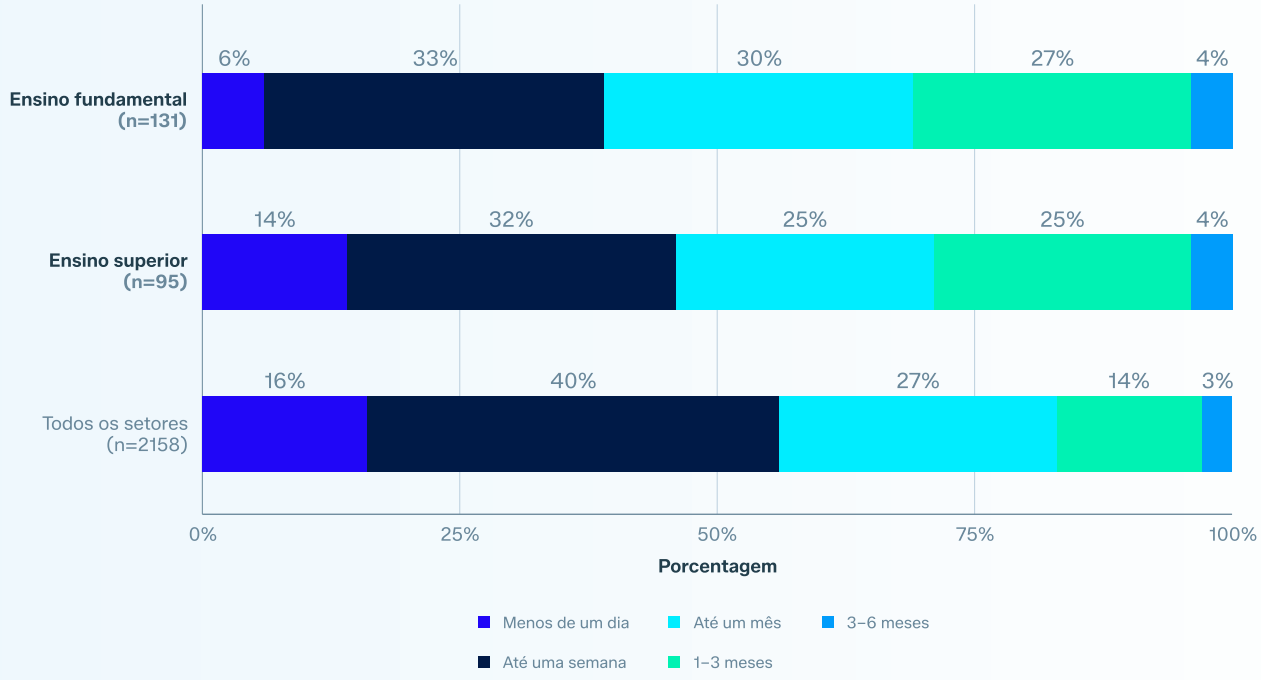
Tempo de recuperação

Os provedores de educação não apenas pagaram mais para se recuperar, como também levaram mais tempo para fazê-lo. A divisão mais nítida está na faixa de recuperação de um a três meses: 27% das instituições de ensino básico e 25% das instituições de ensino superior precisaram desse tempo para se recuperar totalmente, em comparação com apenas 14% da média da pesquisa. **O setor da educação apresentou quase o dobro da probabilidade de enfrentar uma recuperação que durasse um mês ou mais**.

31%

A proporção de instituições de ensino básico que precisaram de pelo menos um mês para se recuperar foi maior do que em qualquer outro setor.

Quanto tempo levou para se recuperar do ransomware



Quanto tempo a sua organização levou para se recuperar por completo do ataque de ransomware? Números de base no gráfico.

A extremidade mais rápida da escala conta a mesma história, só que ao contrário. Apenas 6% das instituições de ensino básico se recuperaram em menos de um dia, em comparação com 16% da média da pesquisa e 14% do ensino superior.

Nenhum setor apresentou uma proporção maior de recuperações prolongadas do que o ensino básico, onde 31% das instituições precisaram de pelo menos um mês para se recuperar totalmente.

Impacto humano do ransomware

O impacto humano sobre as pessoas na área da educação foi maior do que na pesquisa geral, e cada setor da educação sentiu isso de forma diferente. No ensino superior, a pressão determinante veio de cima: 53% das equipes relataram aumento da pressão por parte da alta liderança, 13 pontos percentuais acima da taxa geral da pesquisa, que foi de 40%. Alterações na equipe ou na estrutura organizacional também foram mais comuns no ensino superior (43% contra 32% em todos os setores).

A experiência no ensino básico ficou centrada no reconhecimento e na carga de trabalho. Quase metade das equipes de ensino básico (49%) relataram maior reconhecimento por parte da alta administração, acima da taxa geral da pesquisa, que foi de 36%. O reconhecimento pode ser positivo, mas o aumento da carga de trabalho não é. 43% das equipes de ensino básico relataram um aumento contínuo na carga de trabalho, em comparação com 31% entre os outros setores. A atenção tem dois lados: mais visibilidade, mas também uma carga mais pesada e constante.

53%

A porcentagem de equipes de TI e segurança do ensino superior que enfrentaram maior pressão por parte da alta administração após um ataque, em comparação com 40% na pesquisa geral.

Impacto humano do ransomware

Repercussão	Ensino fundamental (n=81)	Ensino superior (n=51)	Todos os setores (n=1.214)
Aumento em ansiedade e estresse sobre ataques futuros	40%	33%	41%
Aumento da pressão por parte dos líderes seniores	48%	53%	40%
Aumento do reconhecimento pelos líderes seniores	49%	29%	36%
Mudanças na estrutura organizacional/da equipe	33%	43%	32%
Mudança das prioridades/ foco da equipe	33%	35%	32%
Sentimento de culpa porque o ataque não foi interrompido	31%	25%	31%
Aumento contínuo na carga de trabalho	43%	31%	31%
Licença de pessoal devido a problemas de estresse e saúde mental	40%	39%	29%
A liderança da equipe foi substituída.	27%	29%	21%

Qual a repercussão que o ataque de ransomware teve nas pessoas em sua equipe de TI e segurança cibernética, se alguma?
Base: organizações que tiveram dados criptografados. Números de base no gráfico.

O bem-estar dos funcionários foi prejudicado em ambos os segmentos. 39% das equipes do ensino superior e 40% das equipes do ensino básico relataram ausência de funcionários devido ao estresse ou a problemas de saúde mental, bem acima da taxa geral da pesquisa de 29%.

A rotatividade de liderança também aumentou, com 29% das equipes do ensino superior e 27% das equipes do ensino básico tendo sua liderança substituída após o ataque, em comparação com 21% em geral.

Recomendações

Reforce a segurança da identidade como uma defesa contra ransomware. 73% das vítimas de ransomware no setor educacional confirmaram que o incidente de ransomware sofrido foi o mesmo que o ataque de identidade mais significativo que sofreram, uma porcentagem maior do que os 67% da pesquisa geral, o que reforça a forte ligação entre comprometimento de identidade e ransomware nesse setor. Os provedores de educação devem priorizar a detecção e resposta a ameaças de identidade (ITDR), impor a autenticação multifator em todos os pontos de acesso e auditar regularmente as credenciais de identidade, tanto humanas quanto não humanas.

Habilite a autenticação multifator (MFA) de forma abrangente, especificamente a MFA resistente a phishing. A pesquisa mostrou que 98% dos provedores de educação com credenciais comprometidas haviam habilitado a autenticação multifator (MFA) de alguma forma no momento do ataque, mas suas taxas de criptografia ainda eram altas. A autenticação multifator (MFA) por si só não é suficiente para impedir ataques, sendo necessário habilitá-la de forma abrangente, em vez de deixá-la ativada apenas para aplicativos SaaS que a exigem e desativada para logins de VPN, painéis do administrador de firewall e aplicativos legados.

Reforce a proteção de endpoints para modelos de IA fronteiriça. Embora o relatório indique uma queda nos relatos de vulnerabilidades exploradas, os especialistas da Sophos preveem um aumento nos exploits, visto que as organizações têm dificuldades para acompanhar as correções para as vulnerabilidades descobertas pela IA fronteiriça. Ter defesas robustas nos endpoints que bloqueiem automaticamente ataques baseados em exploits é essencial.

Recorra ao suporte especializado ou MDR. A falta de capacidade, habilidades e conhecimento especializado é um tema recorrente em toda a educação, sendo especialmente aguda no ensino superior, onde a falta de conhecimento especializado interno se destacou como uma fragilidade crucial. Lidar com ameaças aprimoradas por IA exercerá ainda mais pressão sobre essas áreas, à medida que as equipes de segurança tentam se manter atualizadas com a tecnologia de IA em rápida evolução. A menos que você tenha confiança em sua capacidade de formar uma equipe interna de operações de segurança, procure um especialista externo para preencher essa lacuna, seja um fornecedor de MDR disponível 24 horas por dia, 7 dias por semana, ou um provedor de serviço gerenciado. Os fornecedores que resolvem mais incidentes de ponta a ponta com IA e automação atuam como um multiplicador de forças, ajudando a reduzir as lacunas de habilidades e capacidade.

Invista em infraestrutura de backup e recuperação. Os backups foram o método de recuperação mais utilizado tanto no ensino básico quanto no ensino superior (77% e 69%, respectivamente, ambos acima da pesquisa geral). Os backups devem ser testados regularmente, armazenados offline ou em formatos imutáveis e integrados a um plano de resposta a incidentes documentado que possa ser executado sob pressão.

Mantenha programas de gerenciamento de exposição. As vulnerabilidades exploradas continuam sendo um importante vetor de ataque e provavelmente aumentarão à medida que os modelos de IA fronteiriça encontrarem novas fragilidades mais rapidamente. As instituições de ensino devem manter uma frequência rigorosa de aplicação de patches e concentrar-se em medidas de mitigação, incluindo segmentação, Zero Trust Network Access e implementações de MFA/autenticação contínua.

Reduza a exposição através do firewall e utilize a telemetria do firewall para detectar ataques precocemente. Os dados de 2026 mostraram que os firewalls são eficazes na detecção de sinais de ransomware, com 65% deles possuindo dados suficientes para identificar um ataque antes que o ransomware fosse detonado. Mas mesmo nesses casos de detecção precoce, as vítimas na área da educação ainda tiveram seus dados criptografados em 51% das vezes, porque o firewall muitas vezes não consegue confirmar ou impedir um ataque sem telemetria de outros pontos de controle. Garanta que seu firewall receba atualizações rápidas o ideal seria recebê-las automaticamente e minimize serviços expostos à internet, como acesso administrativo e portais do usuário. Conecte firewalls ao XDR e ao MDR para que a telemetria do firewall ajude a detectar ataques de ransomware antes que as cargas sejam implantadas. A solução está em um sistema de defesa de segurança cibernética em que os controles compartilhem sinais.

Ações recomendadas em resumo:

1. Segmentação para retardar os invasores
2. ZTNA para substituir VPNs legadas e conter explorações em aplicativos
3. Detecção e resposta a ameaças à identidade (ITDR) para fortalecer a infraestrutura de identidade
4. MFA resistente a phishing como destino, não como ponto de partida
5. Aplicação disciplinada de patches em dispositivos conectados à internet
6. Detecção e resposta 24/7

Conclusão

O Estado do Ransomware na Educação 2026 revela um cenário de ameaças em transição.

Há sinais de progresso: as exigências de resgate estão diminuindo, a recuperação baseada em backup aumentou para níveis próximos aos recordes e os pagamentos de resgate por parte das instituições de ensino são baixos em comparação com outros setores.

Ainda assim, os desafios que permanecem são significativos. Mais da metade dos ataques de ransomware contra instituições de ensino ainda conseguem criptografar dados, os custos médios de recuperação chegam a US$ 2,26 milhões por incidente (valor superior à média da pesquisa) e as instituições de ensino básico apresentaram a maior parcela de recuperações que duraram um mês ou mais.

A identidade é onde se concentra a exposição da educação. Uma parcela maior de provedores de educação confirmou que seu incidente de ransomware foi o mesmo que o ataque de identidade mais significativo que sofreram, em comparação com a pesquisa geral. Para um setor em que a recuperação já é mais lenta e dispendiosa, essa forte interligação faz da infraestrutura de identidade o investimento mais acertado.

Os provedores de educação também precisam se preparar para o desafio decisivo de segurança cibernética da próxima década: As ameaças aumentadas por IA. Os dados já indicam o por quê: 62% das organizações educacionais citaram uma falha de segurança, conhecida ou desconhecida, como um fator em seu ataque, e 63% apontaram para a falta de pessoal ou de habilidades. Ambas as lacunas tornam-se mais relevantes à medida que a IA acelera a velocidade e a escala dos ataques, com os adversários usando a IA para encontrar vulnerabilidades mais rapidamente e orquestrar ataques a múltiplos pontos de controle na velocidade da máquina.

Os dados sobre as causas principais deste ano também revelam um sinal mais profundo. A combinação de causas primárias está se equilibrando; entre todos os setores, incluindo a educação, nenhum vetor isolado predomina. Isso torna arriscado concentrar as defesas de forma muito restrita em uma única causa raiz, porque os atacantes estão obtendo sucesso por meio de multivetores.

O padrão observado nas descobertas deste ano, especialmente no baixo impacto da detecção por firewall e da ativação da MFA nos resultados, aponta para uma direção consistente: quando as defesas operam em isolamento, você não está protegido. Reduzir a lacuna nos ataques da era da IA dependerá menos da adição de mais ferramentas e mais da conexão das que já existem, para que o contexto, a detecção e a resposta possam acompanhar a velocidade exigida pelas ameaças atuais.

Os provedores de educação que terão melhor desempenho contra o ransomware nos próximos anos serão aqueles que mantiverem a atenção da alta administração neste assunto, adotando sistemas de defesa integrados e baseados em IA, investindo não apenas em tecnologia e processos, mas também nas pessoas que, diariamente, defendem contra essas ameaças.

SOPHOS

Para saber mais sobre ransomware e como a Sophos pode ajudar a defender a sua organização, visite nosso site.

Vendas na América Latina
E-mail: latamsales@sophos.com

Vendas no Brasil
E-mail: brasil@sophos.com

2026-09-12 PTBR (DD)