SOPHOS

O ESTADO DO RANSOMWARE NAS CORPORAÇÕES 2025

Resultados de uma pesquisa independente com 1.733 líderes de TI e segurança cibernética em organizações corporativas que foram atingidas por ransomware no último ano.

Documento técnico Sophos. Dezembro, 2025

Apresentação

Bem-vindos ao relatório inaugural da Sophos, O Estado do Ransomware nas Corporações, que expõe a realidade dos ransomwares para as grandes organizações corporativas (1000 ou mais funcionários) em 2025.

O relatório deste ano revela como as experiências com ransomware das organizações corporativas, tanto causas como consequências, evoluíram no último ano. Também elucida fatores operacionais que deixaram as organizações corporativas expostas aos ataques e o impacto humano dos incidentes nas equipes de TI e segurança cibernética.

Baseado em experiências reais de 1.733 líderes de TI e segurança cibernética distribuídos em 17 países e cujas organizações foram atingidas por ransomware no último ano, o relatório oferece insights únicos sobre:

- Por que as organizações corporativas se tornam vítimas de ransomware.
- O que acontece aos dados.
- Pedidos de resgate e pagamentos.
- Impacto comercial do ransomware.
- Impacto humano do ransomware.

Sobre a pesquisa

O relatório se baseia em levantamentos feitos de uma pesquisa independente e totalmente desvinculada encomendada pela Sophos sobre as experiências organizacionais com ransomwares. Uma empresa terceirizada especializada realizou a pesquisa entre janeiro e março de 2025. Todos os entrevistados trabalham em organizações corporativas com entre 1.000 e 5.000 funcionários e foram solicitados a responder com base na experiência que tiveram nos 12 meses anteriores.

Os 1.733 entrevistados das corporações que contribuíram para este relatório estavam distribuídos em 17 países e 14 setores, assegurando que os resultados do estudo reflitam a grande diversidade e abrangência de experiências. O relatório inclui comparações ano a ano, justapondo os resultados de dados capturados em nossas pesquisas anteriores. Todos os dados financeiros são expressos em dólares americanos.

Observação sobre a data dos relatórios

Para facilitar a comparação de dados entre nossas pesquisas anuais, acrescentamos o ano em que a pesquisa foi realizada ao nome do relatório, que, no caso, é 2025. Estamos cientes de que os entrevistados compartilharam conosco suas experiências relativas ao ano anterior, portanto, muitos dos ataques e impactos citados ocorreram em 2024.

Principais descobertas

Por que as organizações corporativas se tornam vítimas de ransomware

- A **exploração de vulnerabilidades** é a causa técnica primária mais comum dos ataques, usada em 29% dos incidentes. **Phishing** e **credenciais comprometidas** seguiram logo atrás, cada qual mencionada em 21% dos incidentes.
- Fatores multioperacionais contribuem para que as organizações corporativas sejam vítimas de ransomware, sendo o mais comum **uma lacuna de segurança desconhecida**, citado por 40% das vítimas, seguido bem de perto por **falta de pessoas/capacidade** e **falta de expertise**, fatores que contribuíram para 39% dos ataques.

O que acontece aos dados

- A taxa de criptografia de dados nas organizações corporativas atingiu o seu nível mais baixo em cinco anos, com **49% dos ataques resultando na criptografia de dados**, valor inferior ao pico de 64% em 2022.
- 30% das corporações que tiveram dados criptografados também passaram pela exfiltração de dados.
- 96% das corporações que tiveram os dados criptografados conseguiram recuperá-los.
- O uso de backups pelas organizações corporativas para restaurar dados criptografados atingiu o seu nível mais baixo dos últimos quatro anos: 53% dos incidentes utilizaram backups.
- 48% das vítimas das corporações **pagaram o resgate** para reaver os dados, ficando entre os mais baixos índices registrados na pesquisa deste ano.

Resgates: exigências e pagamentos

- A média (mediana) do **pedido de resgate** exigido das organizações corporativas caiu 56% no último ano, chegando a **US$ 1,2 milhão** em 2025 em comparação a US$ 2,75 milhões em 2024. O fator primário por trás dessa variação significativa foi a queda de 24% em pedidos de resgate de US$ 5 milhões ou mais: de 38% em 2024 para 29% em 2025. Contudo, é importante notar que houve um aumento de 17% nas demandas entre US$ 1 milhão e US$ 5 milhões.
- A média (mediana) do **resgate pago** pelas organizações corporativas também caiu, chegando a **US$ 1 milhão** em 2025 em comparação a US$ 1,26 milhão em 2024. O declínio se deve em grande parte à queda de 37% dos pagamentos de resgate de US$ 5 milhões ou mais. Contudo, devemos ressaltar que houve um aumento em quase todas as faixas de pagamento abaixo de US$ 5 milhões.
- A **proporção de resgates pagos** pelas corporações caiu de 95% em 2024 para 86% in 2025.
- Examinando em mais detalhes as **exigências versus pagamentos**, quase um terço (31%) das corporações disseram que pagaram o pedido inicial de resgate. 51% pagaram menos do que o valor inicial, enquanto 18% pagaram mais.

Impacto comercial do ransomware

- A média de **custo para as corporações se recuperarem** de um ataque de ransomware caiu 41% no último ano, chegando a **US$ 1,84 milhão** em comparação a US$ 3,12 milhões em 2024.
- Analisando a **velocidade de recuperação**, as organizações corporativas estão se recuperando mais rapidamente, com exatamente metade delas recuperadas em uma semana em 2025 em comparação a 36% em 2024.

Impacto humano do ransomware

Todas as organizações corporativas que tiveram os dados criptografados disseram ter havido repercussões diretas para as equipes de TI e segurança cibernética:

- 40% das equipes de TI e segurança cibernética disseram ter havido **aumento da pressão** pelos líderes seniores, enquanto 31% relataram o **aumento de reconhecimento**.
- 39% relataram **aumento contínuo na carga de trabalho** e **aumento em ansiedade e estresse** sobre ataques futuros.
- 37% registraram uma **mudança de prioridades/foco da equipe**.
- Mais de um terço dos entrevistados (35%) citaram o **sentimento de culpa** porque o ataque não foi interrompido e **mudanças na estrutura organizacional/da equipe** como repercussões do incidente.
- 31% das equipes passaram por períodos de **licença de pessoal** devido a problemas de **estresse e saúde mental** relacionados ao ataque.
- Em mais de um quarto dos casos (27%), as equipes tiveram a **liderança substituída** por causa do ataque.

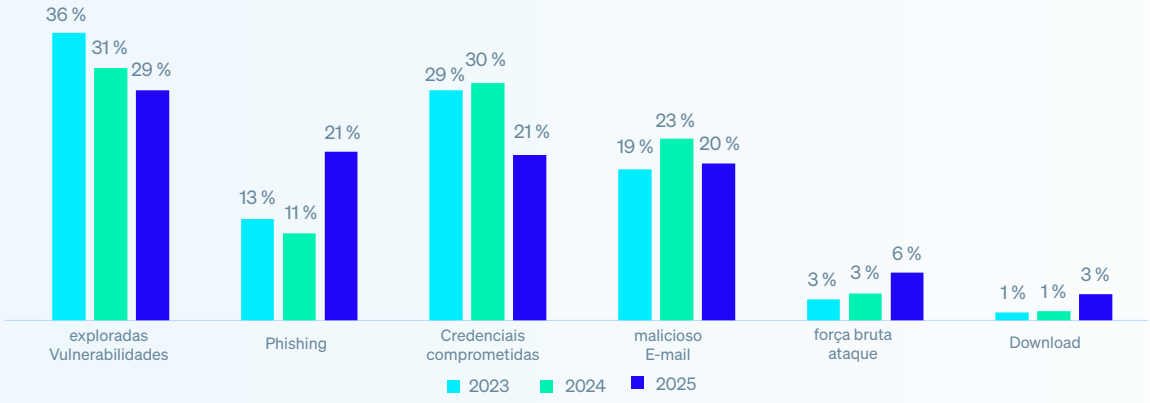
Por que as organizações corporativas se tornam vítimas de ransomware

Causas técnicas primárias dos ataques nas corporações

Por três anos consecutivos, as organizações corporativas apontaram a **exploração de vulnerabilidades** como a principal causa dos ataques de ransomware, responsável por 29% dos incidentes. **E-mails de phishing** ficaram em segundo lugar, subindo de 11% em 2024 para 21% em 2025.

Ataques baseados em credenciais continuam a impor um risco significativo, ainda que os relatos sobre esse vetor de ataque tenham caído significativamente: de 30% em 2024 para 21% em 2025. Por outro lado, as **pequenas e médias empresas** (aquelas com entre 100 e 250 funcionários) citaram os ataques baseados em credenciais como a principal causa primária dos ataques de ransomware, responsáveis por quase um terço (30%) dos incidentes.

Gráfico 1: Causa técnica primária dos ataques de ransomware nas organizações corporativas 2023 – 2025

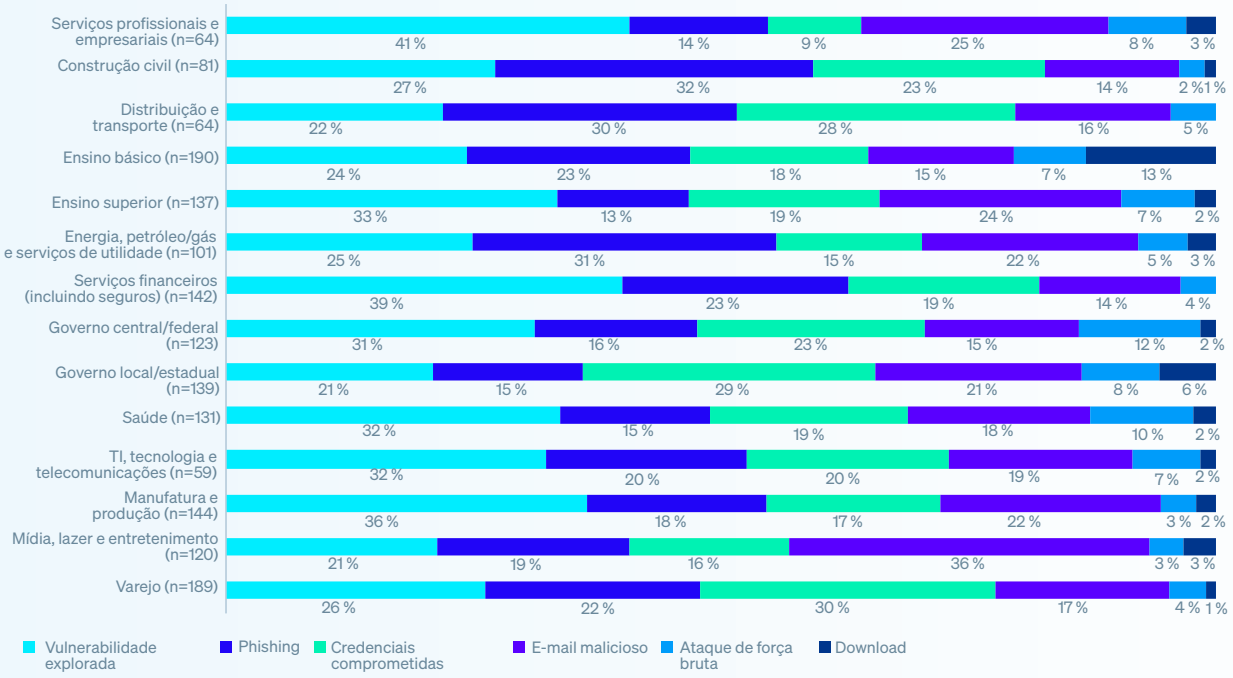


Você sabe a causa primária do ataque de ransomware que a sua organização enfrentou no último ano? Sim. n=1.733 (2025), 1.409 (2024), 1.045 (2023).

A pesquisa revela que as causas primárias variam por setor, mas a exploração de vulnerabilidades é apontada como o maior vetor de ataque às corporações pela maioria dos setores. Vale ressaltar aqui:

- O **phishing** foi a causa primária mais comum citada por fornecedores nos setores de **construção civil** (32%), **distribuição e transporte** (30%) e **energia, petróleo/gás e serviços de utilidade** (31%).
- O **comprometimento de credenciais** foi o vetor de ataque mais observado pelas corporações do **setor varejista**, atribuído a quase um terço dos incidentes (30%).

Gráfico 2: Causa técnica primária dos ataques de ransomware dividida por setor

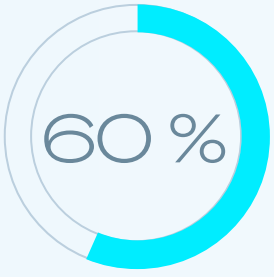


Você sabe a causa primária do ataque de ransomware que a sua organização enfrentou no último ano? Sim. Números de base no gráfico.

Causa organizacional primária dos incidentes nas organizações corporativas

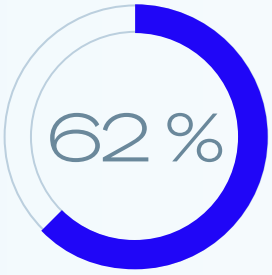
Além das causas técnicas primárias dos incidentes, também é importante entender os fatores organizacionais que deixaram as corporações expostas aos ataques. Os resultados revelam que as vítimas nas organizações corporativas geralmente enfrentam várias dificuldades organizacionais, com os entrevistados citando três fatores, em média, que contribuíram para que se tornassem vítimas do ataque de ransomware.

No geral, as causas organizacionais primárias são distribuídas igualmente entre problemas de proteção, dificuldades com recursos e lacunas de segurança. Contudo, as organizações corporativas estão um pouco mais propensas a apontar a lacuna de segurança (conhecida e desconhecida) como o fator primário.



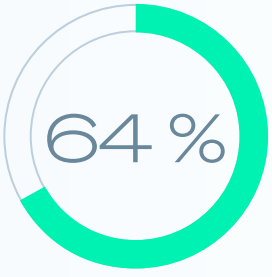
FALTA OU BAIXA QUALIDADE DE PROTEÇÃO

Falta de proteção ou baixa qualidade das soluções de proteção que inviabilizou a interrupção do ataque



FALTA DE PESSOAS/ HABILIDADES

Falta de expertise humana (habilidades ou capacidade) para detectar e interromper o ataque em tempo hábil



LACUNA DE SEGURANÇA (CONHECIDA/DESCONHECIDA)

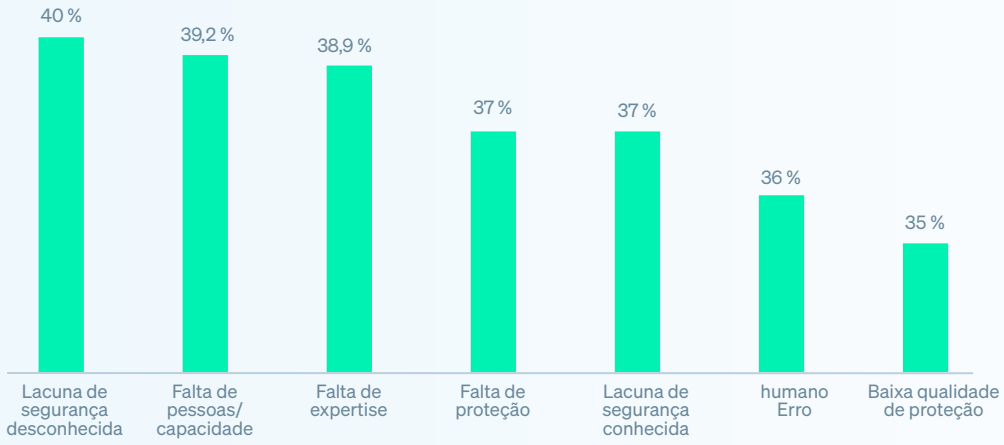
Presença de pontos fracos conhecidos ou desconhecidos em suas defesas

Por que você acha que a sua organização foi vítima de um ataque de ransomware? n=1.733. Respostas consolidadas.

Lacunas de segurança desconhecidas (ou seja, pontos fracos na defesa dos quais os entrevistados não tinham conhecimento) são o motivo mais comum, apontado por 40% dos entrevistados das corporações. De perto, seguem a **falta de pessoas/capacidade** (ou seja, um número insuficiente de peritos em segurança cibernética monitorando os sistemas no momento do ataque) e a **falta de expertise** (ou seja, insuficiência de habilidades ou conhecimento disponível para detectar e bloquear um ataque em tempo hábil), identificadas como fatores contribuintes por 39% das corporações.

Um ponto interessante é que as **PMEs** também identificaram a falta de **pessoas/capacidade** como um fator comum, com 42% apontando este como um fator principal em se tornarem vítimas de um ataque, demonstrando que a escassez de recursos continua a ser um grande desafio geral independentemente do tamanho da organização.

Gráfico 3: Causa operacional primária dos ataques de ransomware nas organizações corporativas



Por que você acha que a sua organização foi vítima de um ataque de ransomware? n=1.733.

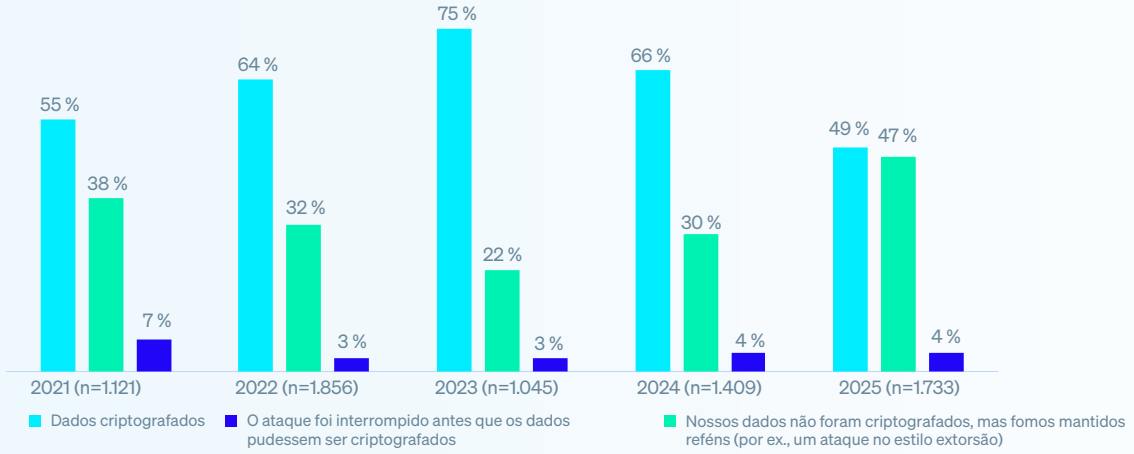
O que acontece aos dados

Criptografia de dados nas corporações

A taxa de criptografia de dados nas organizações corporativas está no seu índice de presença mais abaixo já relatado durante os cinco anos de nossas pesquisas, com menos da metade (49%) dos ataques resultando em dados criptografados, uma queda dos 66% reportados em 2024.

Enquanto isso, a porcentagem de ataques de ransomware que foram bloqueados antes da criptografia de dados mais que duplicou nos últimos dois anos, indo de 22% em 2023 para 47% em 2025. Isso sugere que as organizações corporativas estão ficando mais eficientes em detectar e interromper ataques antes que causem sérios danos.

Gráfico 4: Índice de criptografia de dados em ataques de ransomware nas organizações corporativas 2021 – 2025

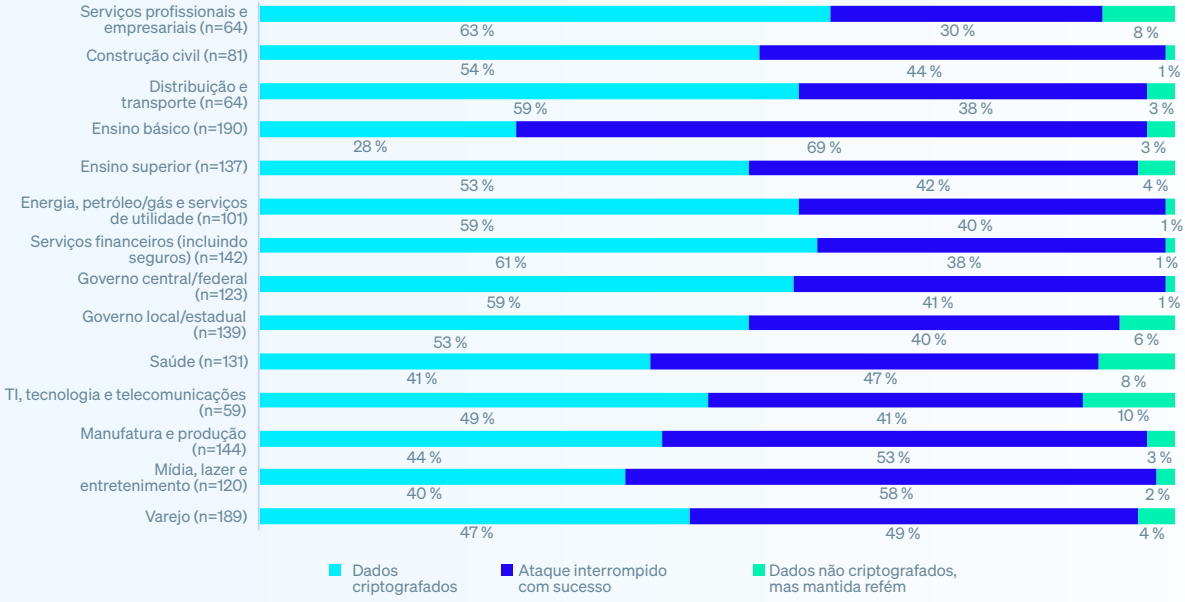


Os criminosos virtuais tiveram sucesso na criptografia de dados da sua organização no ataque de ransomware? Números de base no gráfico.

Índice de criptografia de dados por setor

As corporações do setor de **serviços profissionais e empresariais** estão mais propensas a ter seus dados criptografados (63%), o que indica que as organizações desse setor têm taxas de sucesso mais baixas na detecção e bloqueio de um ataque antes da criptografia e/ou têm menor capacidade de bloquear e reverter a criptografia maliciosa. Enquanto isso, as instituições de **ensino básico** registraram o índice mais baixo de criptografia de dados: 28%.

Gráfico 5: Índice de criptografia de dados nas organizações corporativas por setor



Os criminosos virtuais tiveram sucesso na criptografia de dados da sua organização no ataque de ransomware? Números de base no gráfico.

Roubo de dados

Os adversários não apenas criptografam os dados, eles os roubam. Entre as organizações corporativas, 15% de todas as vítimas de ransomware e 30% das que tiveram seus dados criptografados tiveram seus dados roubados. Ao detalharmos os dados por setor, vemos que:

- Em um extremo, 52% das corporações do setor de **mídia, tecnologia e entretenimento** que passaram pela criptografia de dados também tiveram os dados roubados.
- Já no outro extremo, apenas 11% das corporações no setor de **construção civil** tiveram seus dados roubados além de criptografados.

Ataques no estilo extorsão

Como mostra o gráfico 4, a parcela de corporações que evitou a criptografia de dados, mas que, ainda assim, foi mantida refém manteve-se estável ano a ano, a 4%. Quando analisamos por setor, as organizações de **TI, tecnologia e telecomunicações** foram as mais expostas a esse tipo de ataque: 10%, enquanto as corporações de **construção civil, energia, petróleo e gás e serviços de utilidade, serviços financeiros e governo central/federal** foram as menos afetadas, todas relatando 1%.

No geral, as corporações de **ensino básico** estavam mais capacitadas a prevenir as repercussões de um ataque de ransomware (ou seja, impedir que os dados fossem criptografados, prevenir a exfiltração de dados e evitar sujeitar-se a uma extorsão). Isso sugere que os provedores do ensino básico estão se mostrando supreendentemente eficazes na detecção e intervenção antecipadas, mesmo com seus orçamentos limitados.

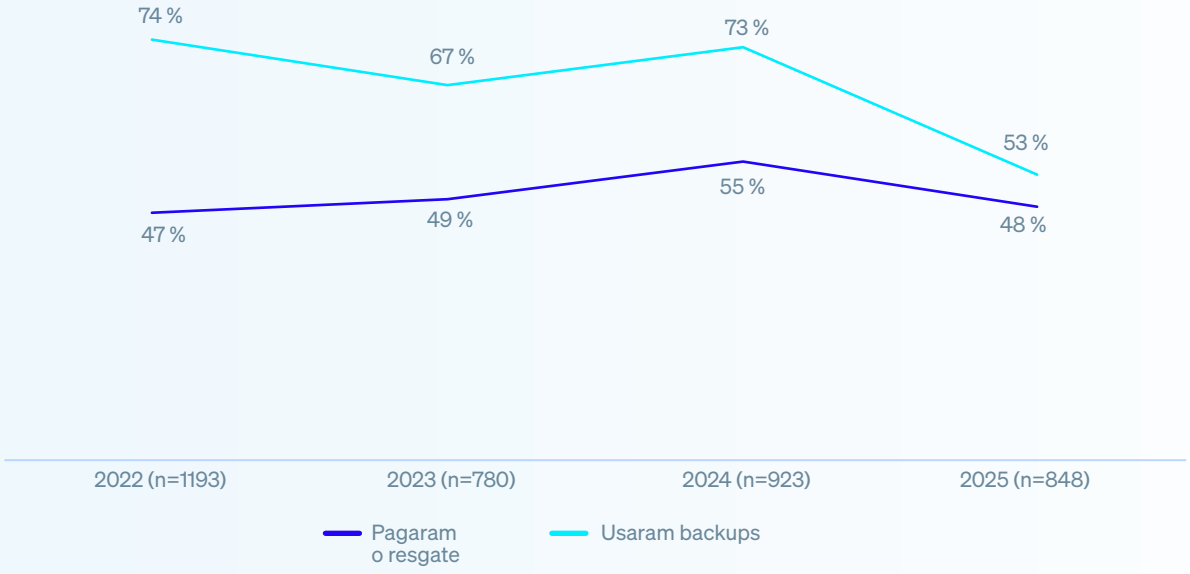
Recuperação de dados criptografados nas organizações corporativas

96% das corporações que tiveram os dados criptografados os recuperaram.

Em 2025, 48% das corporações **pagaram o resgate para recuperar seus dados** — abaixo dos 55% em 2024. Enquanto isso, o **uso de backup** caiu acentuadamente para o índice mais baixo dos últimos quatro anos: 53%, comparado aos 73% em 2024. Coletivamente, esses resultados apontam para uma resistência mais forte às demandas em conjunto com pontos fracos ou falta de confiança na resiliência do backup.

Além disso, a pequena diferença entre as corporações que pagaram o resgate para recuperar os dados e as que usaram backups para recuperar os dados sugere um aumento na dependência de diferentes métodos de recuperação alternativos. Constatamos isso com a revelação de que quase um terço (30%) das corporações que tiveram seus dados criptografados disseram ter **utilizado outro meio para restaurar seus dados**. Métodos alternativos incluem a restauração de cópias de sombra, utilizar recursos de reversão de proteção de endpoint ou recuperar dados de sistemas não afetados.

Gráfico 6: Recuperação de dados criptografados nas organizações corporativas 2021 – 2025



Sua organização conseguiu reaver os dados capturados? Sim, pagamos o resgate e recuperamos os dados; Sim, usamos backups para restaurar os dados. Números de base no gráfico.

Resgates

Pedidos de resgate nas corporações

A média (mediana) do pedido de resgate exigido das organizações corporativas caiu 56% no último ano, chegando a US$ 1,2 milhão em 2025 — bem abaixo dos US$ 2,75 milhões em 2024. A diminuição nos pedidos de resgate direcionados às corporações se deve em grande parte à queda de 24% nas exigências de pagamentos de US$ 5 milhões ou acima feitas no último ano. Contudo, é importante notar que houve um aumento de 17% nas demandas entre US$ 1 milhão e US$ 5 milhões, que computam 27% dos pedidos de resgate — acima dos 23% em 2024.

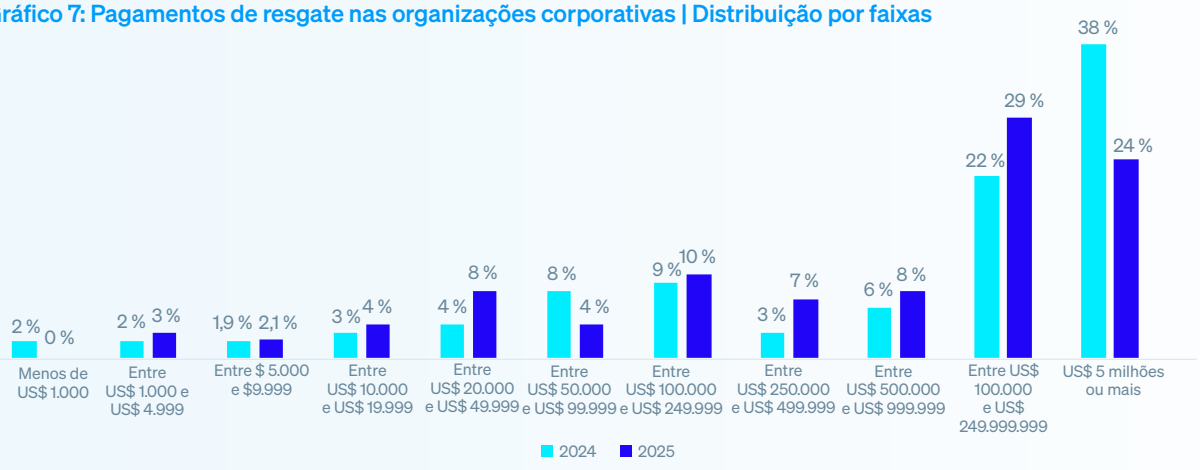
Pagamento de resgate nas corporações

Seguindo essa tendência, a média (mediana) do resgate pago pelas corporações também observou um declínio: de US$ 1,26 milhão em 2024 para US$ 1 milhão em 2025. Isso se deve em grande parte à queda de 37% em pagamentos de US$ 5 milhões ou acima feitos no último ano. Entretanto, o relatório revela um aumento ano a ano em quase todas as faixas de pagamento abaixo de US$ 5 milhões.

Esses padrões sugerem que os golpistas estão deixando para trás os grandes resgates e atacando as corporações com exigências mais medianas, almejando valores que continuam problemáticos, mas que, realisticamente, são bem mais possíveis de serem pagos.

As **PMEs** seguiram um modelo similar, embora a queda em exigências e pagamentos tenha sido ainda mais pronunciada. A mediana de pedidos de resgate e pagamentos caiu acentuadamente, de US$ 2 milhões em 2024 para US$ 126 mil e US$ 200 mil em 2025, respectivamente, reforçando a grande tendência entre os golpistas de readequar suas expectativas por somas mais tangíveis para todos os tamanhos de organizações.

Gráfico 7: Pagamentos de resgate nas organizações corporativas | Distribuição por faixas

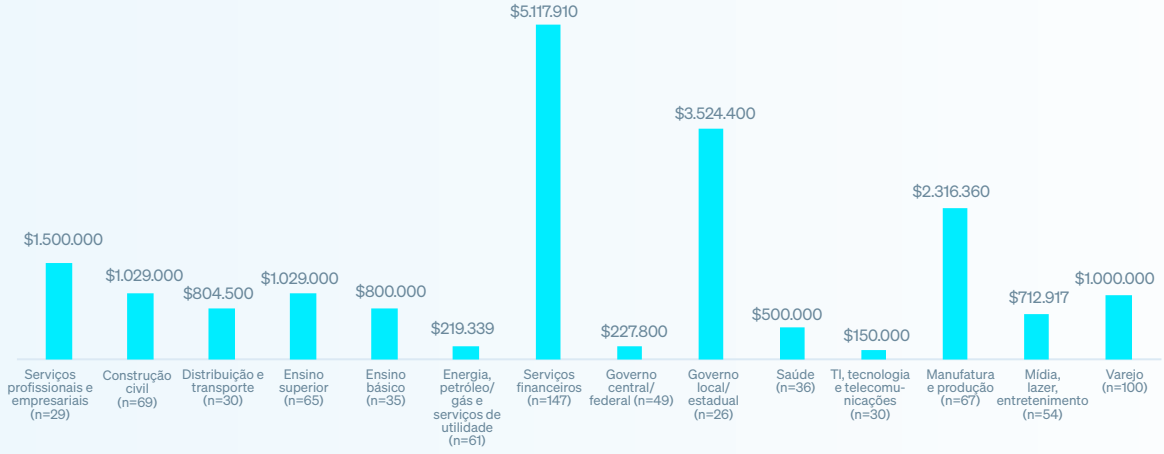


Qual foi o pagamento de resgate que foi efetuado aos invasores? n=414 (2025), 470 (2024)

Pagamentos de resgate por setor

Os pagamentos de resgate variam consideravelmente por setor, com as corporações do setor de serviços financeiros pagando aos invasores a mais alta média (mediana) de resgate: US$ 5,1 milhões. Isso pode ser devido ao alto volume operacional e à baixa tolerância a conturbações, o que deixa os golpistas confiantes de que grandes pagamentos serão um resultado bastante provável.

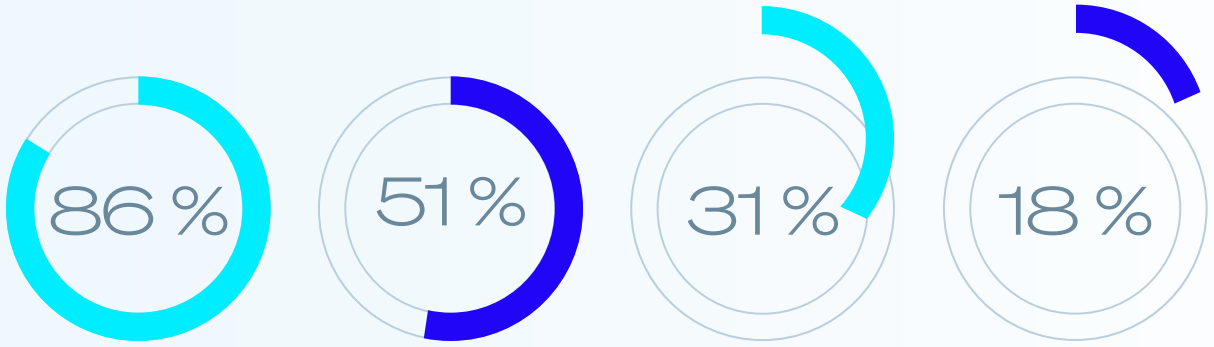
Gráfico 8: Pagamentos de resgate por setor



Qual foi o pagamento de resgate que foi efetuado aos invasores? Números de base no gráfico. Observação: Números de base com menos de 30 resultados devem ser considerados meros indicativos.

Como se parecem os pagamentos reais feitos pelas corporações comparados às exigências iniciais

414 corporações que pagaram o resgate compartilharam conosco os valores inicial e o realmente efetuado, revelando que pagaram, em média, 86% do pedido de resgate inicial, uma queda muito bem-vinda dos 95% registrados em 2024. No geral, 51% pagaram menos do que o pedido inicial, 18% pagaram mais e quase um terço (31%) mantiveram a exigência inicial.



Por que a maioria dos pagamentos de resgate feitos pelas corporações difere do valor inicial exigido

Na pesquisa, também examinamos por que algumas corporações pagam mais do que o resgate inicial exigido e outras pagam menos, ressaltando uma área importante quando lidamos com um ataque de ransomware.

72 corporações que **pagaram mais** do que o resgate inicial revelaram que:

- 61%: os invasores acreditavam que poderíamos pagar mais.
- 49%: os invasores se deram conta de que éramos um alvo de grande valor.
- 42%: nossos backups não funcionaram ou apresentaram defeitos.
- 39%: os invasores se irritaram e aumentaram o preço.
- 31%: não pagamos rápido o suficiente, então o preço subiu.

No geral, as organizações corporativas citaram dois fatores por trás da decisão de pagar mais, revelando os vários desafios que as vítimas enfrentam ao tentar recuperar seus dados.

214 corporações que **pagaram menos** do que a exigência inicial explicaram como conseguiram abaixar o valor do pagamento:

- 49%: negociamos um valor mais baixo com os invasores.
- 46%: pagamos o resgate rapidamente, assim conseguimos um desconto.
- 45%: os invasores reduziram o valor do resgate para nos incentivar a pagar.
- 43%: os invasores reduziram o valor do resgate devido a pressões externas (por exemplo, da mídia ou de autoridades legais).
- 38%: terceiros negociaram um valor mais baixo com os invasores.

Essa coorte também relatou, em média, dois fatores por trás do baixo pagamento de resgate, o que enfatiza ainda mais a complexidade da situação que as vítimas de ransomware enfrentam.

Consequências comerciais do ransomware

Custos de recuperação nas organizações corporativas

A média (mediana) do custo de recuperação de um ataque de ransomware para as corporações (excluindo pagamento de resgate) atingiu o ponto mais baixo dos últimos três anos, marcando uma queda de 41% no ano, de US$ 3,12 milhões em 2024 para US$ 1,84 milhão. O valor também está US$ 330 mil mais baixo do que os US$ 2,17 milhões registrados em 2023.

2023	2024	2025
US$ 2,17 milhões	US$ 3,12 milhões	US$ 1,84 milhões

Qual foi o custo aproximado para a sua organização retificar o impacto do ataque de ransomware mais significativo (considerando-se período de inatividade, tempo de pessoal, custo dos equipamentos, custo da rede, perda de oportunidades etc.), salvo o pagamento de resgate efetuado? n=1.733 (2025), 1.409 (2024), 1.045 (2023)

Quando examinamos a distribuição por setor, observamos que a recuperação varia consideravelmente. As corporações de **ensino básico** registraram o custo médio mais alto para retificar incidentes, US$ 2,66 milhões. Já as corporações no setor de **serviços profissionais e empresariais** registraram o mais baixo custo, US$ 0,92 milhão. Parte dessa diferença é um provável reflexo do nível de infraestrutura de TI vista como necessária para a recuperação após um ataque, com as organizações de ensino básico normalmente utilizando soluções mais antigas do que os provedores de serviços do setor privado.

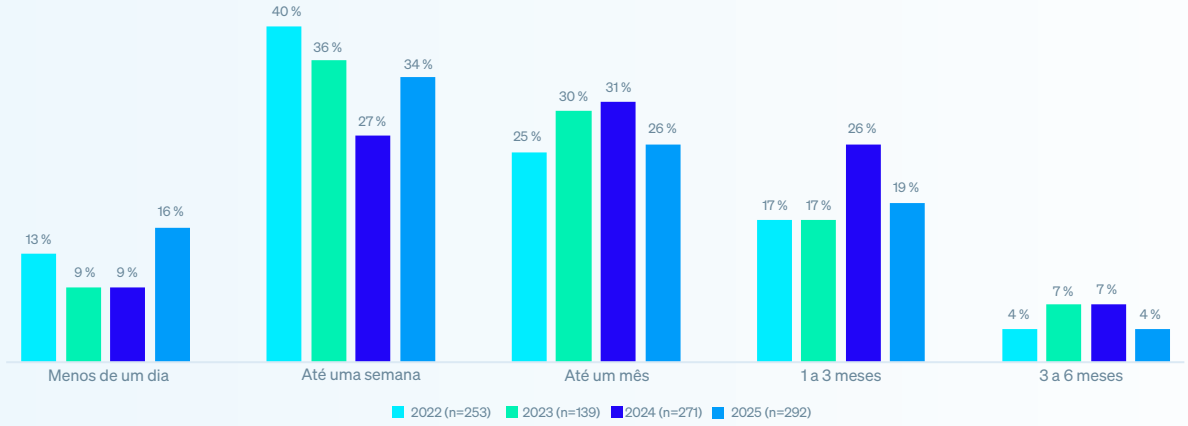
Gráfico 9: Custo de recuperação de ransomware dividido por setor (milhões de USD)

Qual foi o custo aproximado para a sua organização retificar o impacto do ataque de ransomware mais significativo (considerando-se período de inatividade, tempo de pessoal, custo dos equipamentos, custo da rede, perda de oportunidades etc.), excluindo pagamentos de resgate realizados? Números de base no gráfico.

Tempo de recuperação nas organizações corporativas

Os dados revelam que, em 2025, as corporações estão acelerando o tempo de recuperação após ataques de ransomware. Metade se recuperou em uma semana, um aumento dos 36% registrados em 2024. Ao mesmo tempo, a proporção que precisou de um a três meses para se recuperar caiu para 19%, comparado aos 26% registrados em 2024. No geral, 95% das corporações vitimadas se recuperaram completamente em três meses, demonstrando a crescente resiliência e capacidade de recuperação do setor.

Gráfico 10: Tempo de recuperação de ataques de ransomware pelas organizações corporativas 2022 – 2025



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

Consequências humanas do ransomware

A pesquisa deixa claro que ter os dados criptografados em um ataque de ransomware causa repercussões significativas para as equipes de TI e segurança cibernética nas organizações corporativas, com todos os entrevistados dizendo que suas equipes foram afetadas de alguma forma.

Gráfico 13: Consequências às equipes de segurança cibernética e TI por terem os dados criptografados

40 %	Aumento da **pressão** pelos líderes seniores
39 %	Contínuo**aumento de carga de trabalho**
39 %	Aumento em **ansiedade e estresse** sobre ataques futuros
37 %	Mudança das **prioridades/foco da equipe**
35 %	Mudanças na **estrutura** organizacional/da equipe
35 %	Sentimento de **culpa** porque o ataque não foi interrompido
31 %	Licença de pessoal devido a problemas de **estresse e saúde mental**
31 %	Aumento do **reconhecimento** pelos líderes seniores
27 %	A liderança da nossa equipe foi **substituída**

Qual a repercussão que o ataque de ransomware teve nas pessoas em sua equipe de TI e segurança cibernética, se alguma? n=848

Recomendações

Embora as organizações corporativas tenham passado por várias mudanças com relação a ransomwares no último ano, a ameaça continua significante. Os adversários continuam a incrementar os seus ataques, sendo essencial que as equipes e suas defesas cibernéticas acompanhem essa evolução de ransomwares e outras ameaças. Utilize os insights deste relatório para fortalecer as suas defesas, moldar as suas respostas às ameaças e limitar o impacto do ransomware nos seus negócios e nas pessoas. Concentre-se nestas quatro áreas para ficar na dianteira dos ataques:

- **Prevenção**. A defesa de maior sucesso contra um ransomware é aquela em que o ataque nunca acontece, porque os adversários não puderam violar a sua organização. Siga os passos ressaltados neste relatório para eliminar as causas técnicas e operacionais primárias.
- **Proteção**. Uma segurança básica forte é essencial. Endpoints (incluindo servidores) são o destino principal dos agentes de ransomware, portanto, assegure que apresentem uma boa defesa, incluindo proteção dedicada contra ransomware para interromper e reverter a criptografia maliciosa.
- **Detecção e resposta.** Quanto mais cedo um ataque for interrompido, melhor o resultado final. A detecção e resposta a ameaças 24 horas passou a ser um componente essencial da defesa. Se você não tem pessoal interno ou competências para isso, trabalhe com um provedor de MDR confiável para a detecção e resposta gerenciadas.
- **Planejamento e preparo.** Ter um plano de resposta a incidentes implementado e que você conheça muito bem vai melhorar imensamente os resultados caso o pior aconteça e você enfrente um ataque grave. Certifique-se de fazer backups de qualidade e de praticar a restauração dos dados nesses backups com regularidade para se preparar para uma recuperação mais rápida caso você seja atingido.

Para explorar as formas como a Sophos pode ajudar você a otimizar suas defesas contra ransomware, fale com um consultor ou acesse www.sophos.com

Saiba mais sobre ransomware e como a Sophos pode ajudar a defender a sua organização.

A Sophos oferece soluções de segurança cibernética líder do setor para empresas de todos os tamanhos, protegendo-as em tempo real de ameaças avançadas como malware, ransomware e phishing. Com recursos comprovados de última geração, seus dados comerciais ficam protegidos de modo eficiente por produtos que incorporam inteligência artificial e machine learning.

2025-12-08 WP (MP)

SOPHOS