SOPHOS
Cybersecurity evolved.

# O Estado do Ransomware 2021

A pesquisa anual da Sophos sobre ransomware expõe novos insights com base na experiência das organizações de médio porte em todo o globo. Ela explora a prevalência dos ataques, bem como o seu impacto nas vítimas, incluindo tendências ano a ano. Este ano, pela primeira vez, a pesquisa revela também os pagamentos de regaste efetuados pelas vítimas, bem como a proporção de dados que as vítimas foram capazes de recuperar após terem pago o resgate.

*Documento técnico Sophos. Abril, 2021*

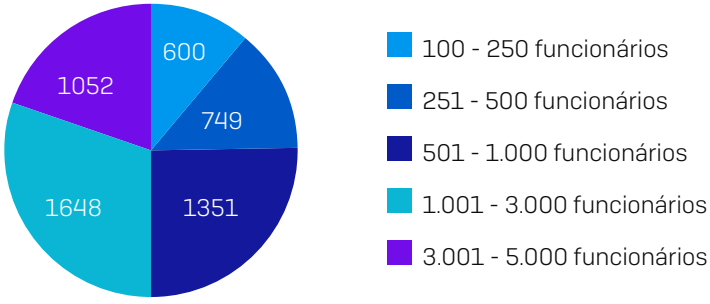
# Sobre a pesquisa

A Sophos encarregou uma firma independente de pesquisa de opinião, a Vanson Bourne, para realizar um estudo com 5.400 tomadores de decisão de serviços de TI em 30 países. A pesquisa foi conduzida em janeiro e fevereiro de 2021.

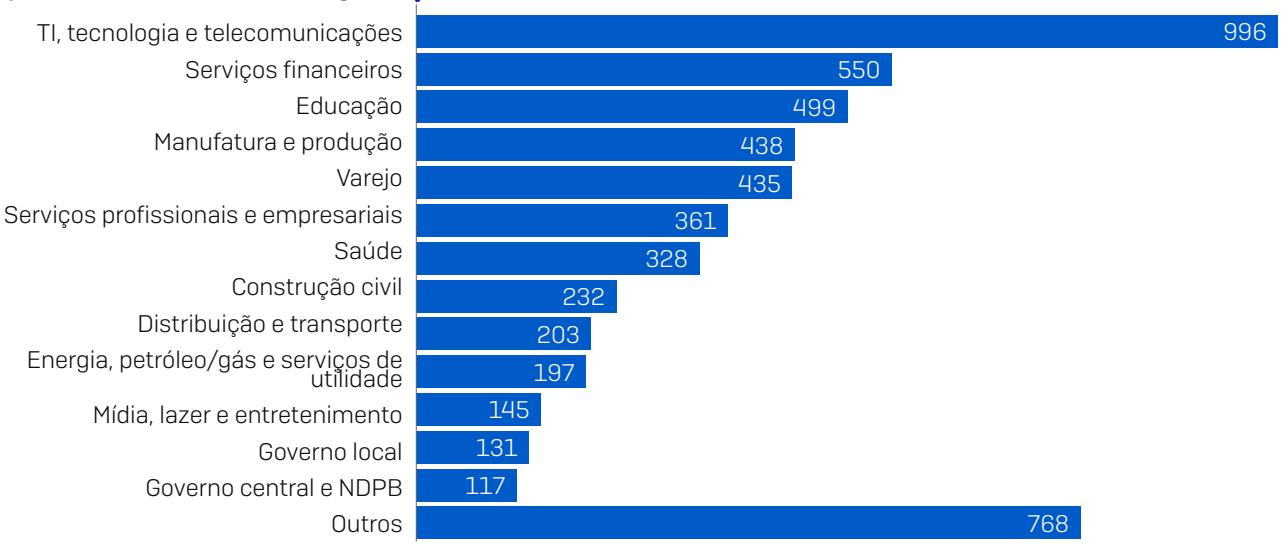
| PAÍS | Nº DE RESPONDENTES | PAÍS | Nº DE RESPONDENTES | PAÍS | Nº DE RESPONDENTES |
|---|---|---|---|---|---|
| Austrália | 250 | Índia | 300 | Arábia Saudita | 100 |
| Áustria | 100 | Israel | 100 | Singapura | 150 |
| Bélgica | 100 | Itália | 200 | África do Sul | 200 |
| Brasil | 200 | Japão | 300 | Espanha | 150 |
| Canadá | 200 | Malásia | 150 | Suécia | 100 |
| Chile | 200 | México | 200 | Suíça | 100 |
| Colômbia | 200 | Países Baixos | 150 | Turquia | 100 |
| República Tcheca | 100 | Nigéria | 100 | EAU | 100 |
| França | 200 | Filipinas | 150 | Reino Unido | 300 |
| Alemanha | 300 | Polônia | 100 | EUA | 500 |

Como nos anos anteriores, 50% dos respondentes de cada país vieram de organizações com entre 100 e 1.000 funcionários e 50% vieram de organizações com entre 1.001 e 5.000 funcionários. Os respondentes também vieram de uma grande diversidade de setores.

### Quantos funcionários a sua organização tem em âmbito global?




### Em que setor se encontra a sua organização?



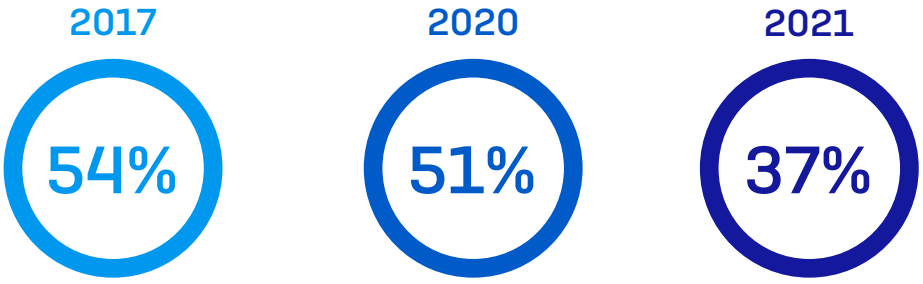
# Principais descobertas

- **37%** das organizações dos respondentes **foram atingidas por ransomware no último ano**
- **54%** das que foram atingidas por ransomware no último ano disseram que os **criminosos cibernéticos tiveram êxito na criptografia dos dados** no ataque mais significativo
- **96%** das que tiveram seus dados criptografados **conseguiram reaver seus dados** no ataque de ransomware mais significativo
- A **média de resgate pago** pelas organizações de médio porte foi **US$ 170.404,00**
- Porém, em média, apenas **65% dos dados criptografados foram recuperados** após o pagamento do resgate
- A **conta média para retificar um ataque de ransomware**, considerando-se período de inatividade, tempo de pessoal, custo dos equipamentos, custo da rede, perda de oportunidades, resgate pago e outros fatores, foi de **US$ 1,85 milhão**
- Os **ataques no estilo extorsão**, em que os dados não são criptografados, mas a vítima ainda assim é mantida como refém, **mais que duplicaram** desde o ano anterior, subindo de 3% para 7%
- Ter **pessoal de TI treinado que seja capaz de parar os ataques** é o motivo mais comum de algumas organizações estarem confiantes de que não serão atingidas por ransomware no futuro

# A prevalência do ransomware

## Ransomware continua a ser uma ameaça de peso

37% das organizações – mais de um terço das 5.400 entrevistadas – foram atingidas por ransomware no último ano, especificamente definido como **vários computadores impactados por um ataque de ransomware, mas não necessariamente criptografados**. Ainda que seja um número alto, a boa notícia aqui é que essa foi uma redução significativa em comparação ao ano anterior, quando 51% disseram ter sido atingidas.

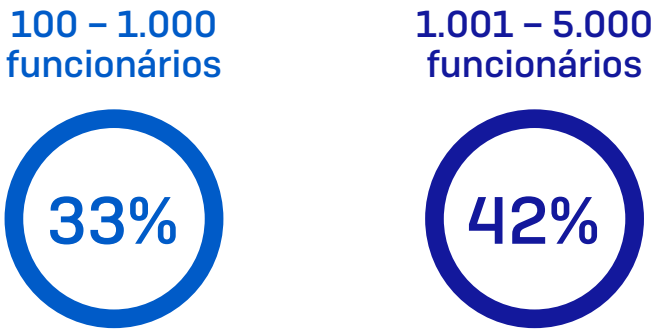



*Sua organização foi atingida por ransomware neste último ano? Sim [2021=5.400; 2020=5.000; 2017=2.700], omitindo algumas opções de resposta, dividido por ano*

Mudanças no comportamento dos invasores observadas pelo SophosLabs e pelas equipes do Sophos Managed Threat Response indicam que a redução no número de ataques pode ser devida em parte à evolução das abordagens de ataque. Por exemplo, muitos invasores mudaram dos ataques automatizados generalizados e em grande escala para ataques mais direcionados que incluem a manipulação fraudulenta realizada por humanos com as mãos no teclado. Enquanto o número de ataques em geral está menor, nossa experiência mostra que o potencial para danos desses ataques direcionados é muito maior.

## Grandes organizações estão mais propensas a serem atingidas

Analisando o número de incidentes de ransomware pelo tamanho da organização, observamos que as grandes organizações registraram uma grande prevalência de ataques, com 42% do grupo com 1.001 a 5.000 funcionários admitindo terem sido atingidas em comparação com 33% de empresas menores.

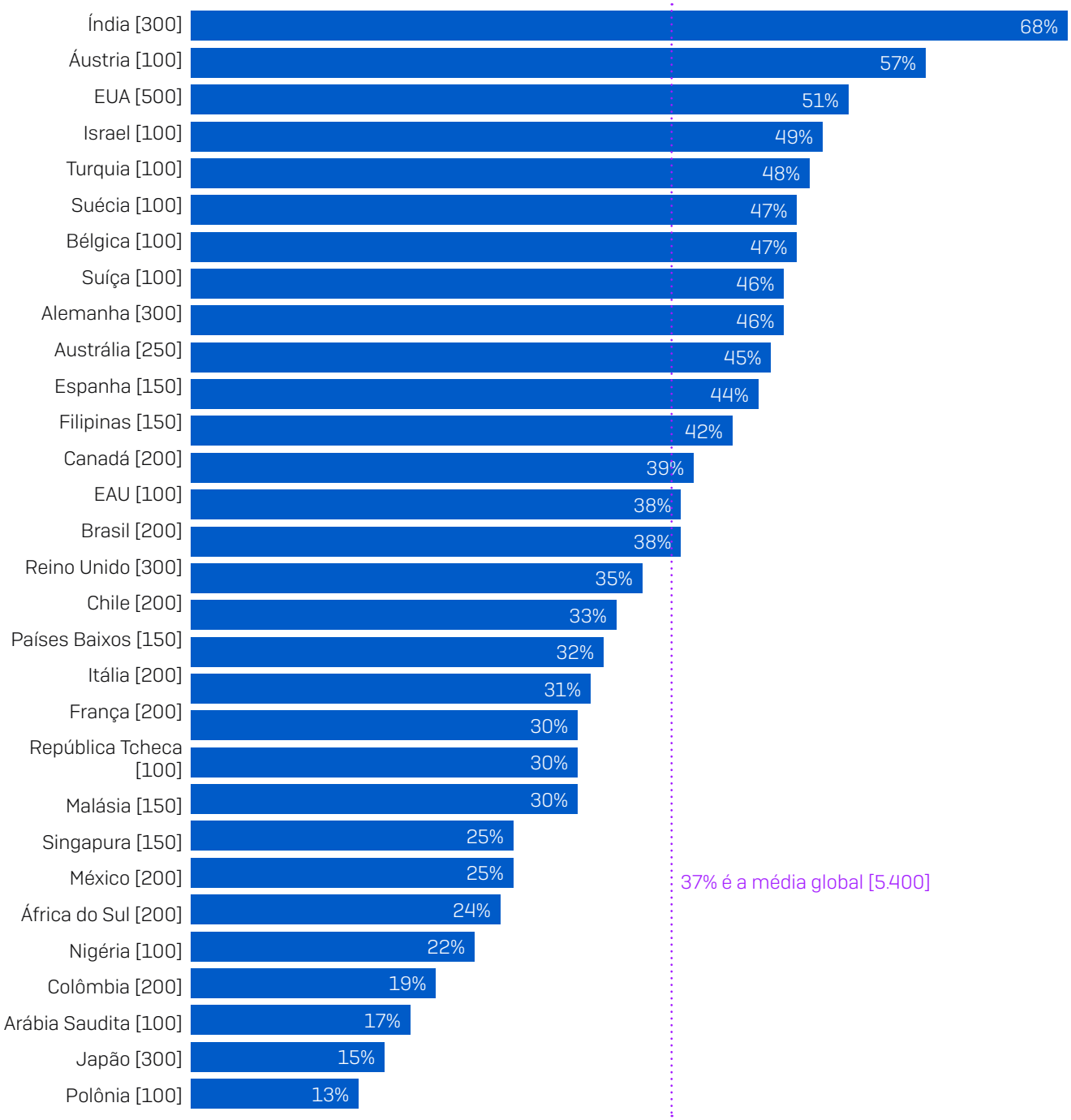



*Sua organização foi atingida por ransomware neste último ano? Sim [5.400], omitindo algumas opções de resposta, dividido por tamanho da organização*

Este ano, a lacuna entre as pequenas e grandes organizações também aumentou de sete pontos percentuais em 2020 para nove pontos percentuais. O aumento do foco de ataque em organizações maiores não surpreende: empresas maiores estão mais propensas a ter mais dinheiro, portanto um alvo mais lucrativo. Com isso, uma em cada três organizações menores foi atingida por ransomware no último ano, confirmando que elas permanecem na mira dos invasores. Aqui não há vencedores.

## Níveis de ataques variam pelo globo

A análise dos dados baseada no país em que o respondente está situado revela resultados interessantes.




*Sua organização foi atingida por ransomware neste último ano? Sim [números de base no gráfico], omitindo algumas opções de resposta, dividido por país*

A **Índia** encabeça a lista, com 68% dos respondentes registrando que foram atingidos por ransomware no ano passado. Enquanto os agentes de ransomware que fazem manchetes nos noticiários estão normalmente na China, Coreia do Norte, Rússia e outros países do bloco da antiga União Soviética, o SophosLabs constata altos índices de ransomware doméstico na Índia, ou seja, adversários indianos atacando empresas indianas.

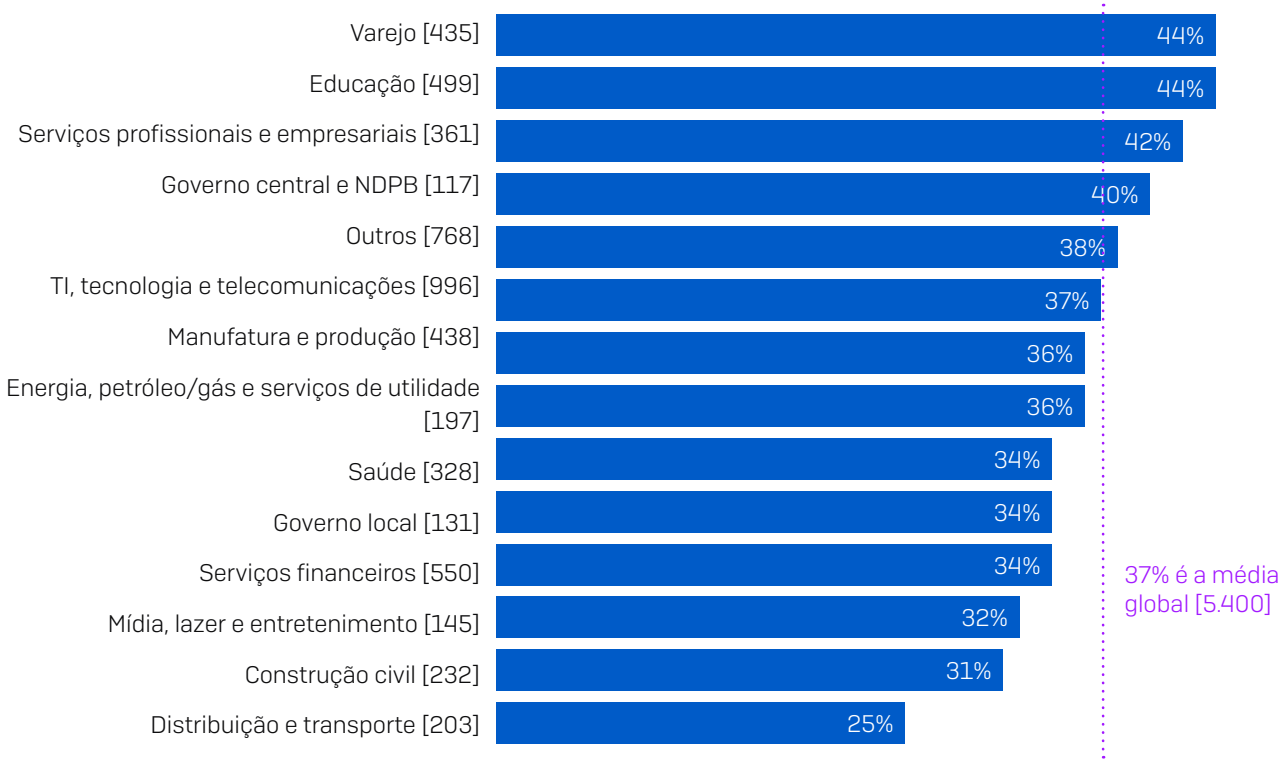
Os **EUA** são um alvo muito popular entre os criminosos cibernéticos, pois são vistos pelo seu potencial de altas demandas de resgate, com apenas um pouco mais da metade – 51% – dos respondentes nos EUA dizendo ter sido atingidos no ano passado.

**Polônia, Colômbia, Nigéria, África do Sul** e **México** registram uns dos mais baixos níveis de ataque, provavelmente em consequência do baixo PIB, o que resulta em um baixo potencial de resgate para os invasores.

O **Japão** se destaca como uma economia desenvolvida com baixíssimos índices de ransomware – apenas 15% dos respondentes mencionaram ter sido atingidos por ransomware no ano passado. Tradicionalmente, o Japão registra baixíssimos índices de ransomware em nossas pesquisas anuais. Talvez seja porque as organizações japonesas investiram pesado nas defesas anti-ransomware, ou porque a natureza única do idioma japonês faça delas um alvo mais difícil para os adversários.

## Varejo e educação sofrem a maioria dos ataques de ransomware

Examinando o índice de ataques por setor, observamos variações consideráveis na propensão de ser atingindo por ransomware entre diferentes setores.




*Sua organização foi atingida por ransomware neste último ano? Sim [números de base no gráfico], omitindo algumas opções de resposta, dividido por setor*

**Varejo** e **educação** exibiram o mais alto índice de ataques, com 44% dos respondentes nesses setores registrando que foram atingidos.

**Saúde**, que geralmente está nas manchetes devido a ataques de ransomware, acabou por registrar níveis ligeiramente abaixo dos índices médios de ataques, com 34% dos respondentes dizendo que suas organizações foram atingidas. A constante exposição do setor nos noticiários provavelmente deve-se às obrigações legais que exigem que as organizações de saúde revelem um ataque, enquanto muitas das organizações comerciais podem manter o fato privado.

# O impacto dos ransomwares

## Criptografia em queda. Extorsão em alta.

Perguntamos às organizações atingidas por ransomware se os criminosos obtiveram êxito na criptografia dos dados: 54% disseram sim. Outras 39% foram capazes de parar o ataque antes que seus dados pudessem ser criptografados, enquanto 7% disseram que seus dados não foram criptografados, mas ainda assim foram sequestrados.

Quando comparamos esses números com os resultados obtidos da nossa pesquisa de 2020, uma história bastante interessante se destaca.

| 2020 | 2021 | |
|---|---|---|
| 73% | 54% | Criminosos criptografaram dados com êxito |
| 24% | 39% | Ataque interrompido antes que os dados pudessem ser criptografados |
| 3% | 7% | Dados não criptografados, mas a vítima continua refém |

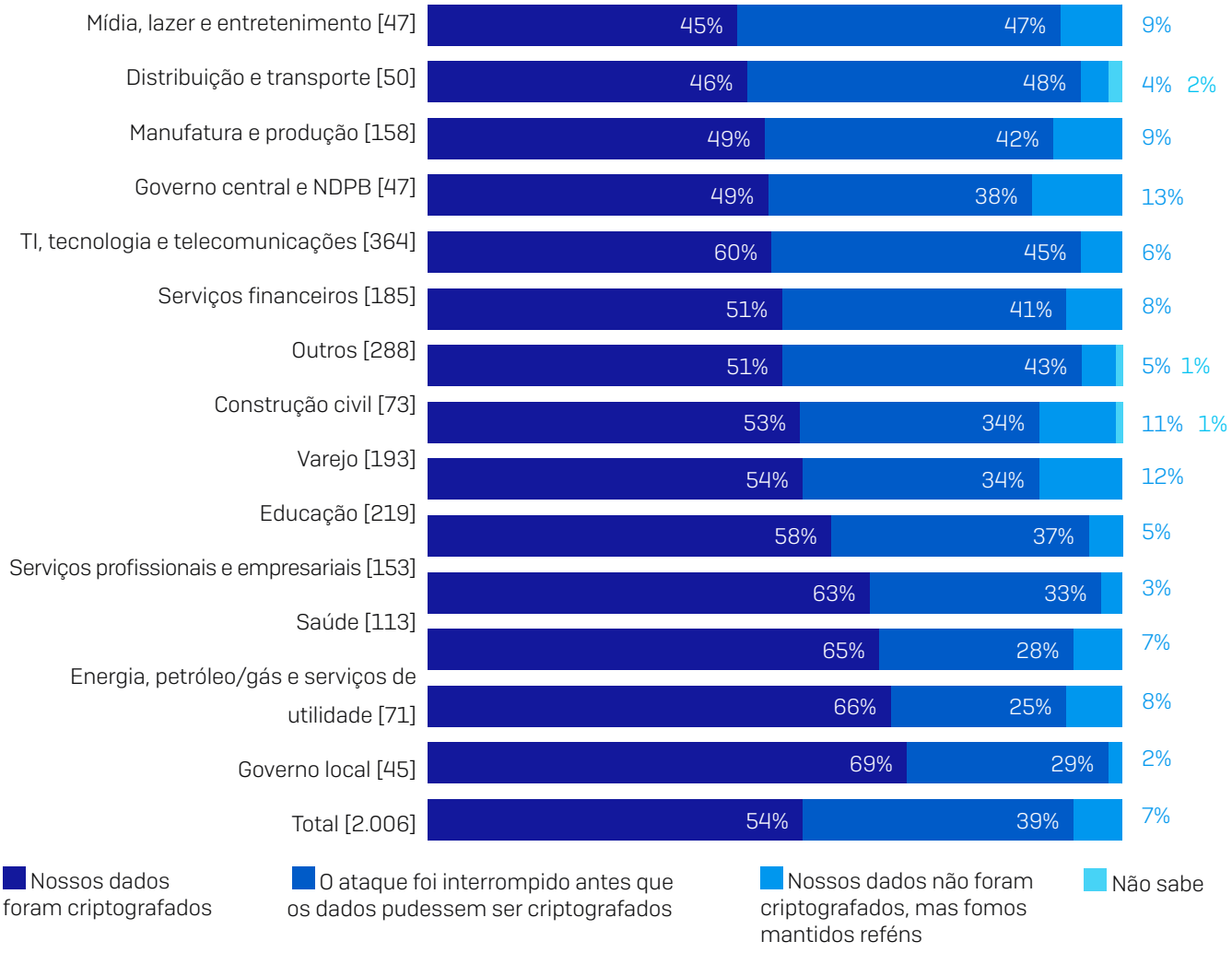
*Os criminosos virtuais tiveram sucesso na criptografia de dados da sua organização nos ataques de ransomware mais significativos? [2021=2.006, 2020=2.538] organizações que foram atingidas por ransomware no último ano*

Primeiramente, no último ano, houve uma queda percentual acentuada de ataques em que os criminosos tiveram êxito na criptografia dos dados: de 73% para 54%, com muitas outras organizações agora capazes de parar o ataque antes que os dados possam ser criptografados. Isso indica que a adoção da tecnologia anti-ransomware está valendo a pena.

Contudo, vemos também que a porcentagem de ataques em que os dados não foram criptografados, mas a vítima foi feita refém, mais que dobraram. Alguns invasores estão mudando para os ataques no estilo extorsão, em que, ao invés de criptografar arquivos, eles os roubam e depois ameaçam publicar os dados a menos que o resgate exigido seja pago. Isso requer menos esforços da parte deles – não precisam criptografar nem descriptografar. Os adversários geralmente equiparam o valor das multas por violação de dados em suas exigências, em uma tentativa a mais de forçar suas vítimas a pagar.

## Capacidade de interromper a criptografia varia imensamente entre setores

Quando se trata de interromper a criptografia de arquivos, alguns setores se saem melhor do que outros.




*Os criminosos virtuais tiveram sucesso na criptografia de dados da sua organização nos ataques de ransomware mais significativos? [números de base no gráfico] organizações que foram atingidas por ransomware no último ano*

**Distribuição e transporte** é o setor com melhor capacidade de interromper a criptografia de dados pelos invasores (48%), seguido de perto por **mídia, lazer e entretenimento** (47%).

De modo recíproco, **governo local** é o setor em que as organizações estão mais propensas a ter seus dados criptografados em um ataque de ransomware (69%). Isso provavelmente é resultado de uma maleficência dupla:

- Defesas mais fracas: em geral, as organizações governamentais locais lutam com orçamentos de TI baixos e pessoal de informática sobrecarregado ou limitado.
- Maior foco do invasor: devido ao seu tamanho e ao acesso a fundos públicos, as organizações governamentais são frequentemente vistas como alvos lucrativos, sendo foco de ataques mais sofisticados.
  Além disso, como veremos mais adiante, o governo local também é o setor com maior propensão a pagar o resgate.

**Governo central e órgãos públicos não departamentais (NDPB)** é o setor mais propenso a passar por uma extorsão (13%).

**Saúde**, como vimos, está abaixo da média em relação ao número de ataques sofridos. Entretanto, os invasores obtêm êxito na criptografia de arquivos em quase dois terços (65%) dos incidentes, o que está consideravelmente acima da média.

## Mais vítimas estão pagando o resgate

Perguntamos às organizações cujos dados foram criptografados (1.086) se elas conseguiram reaver seus dados e como, em caso positivo.

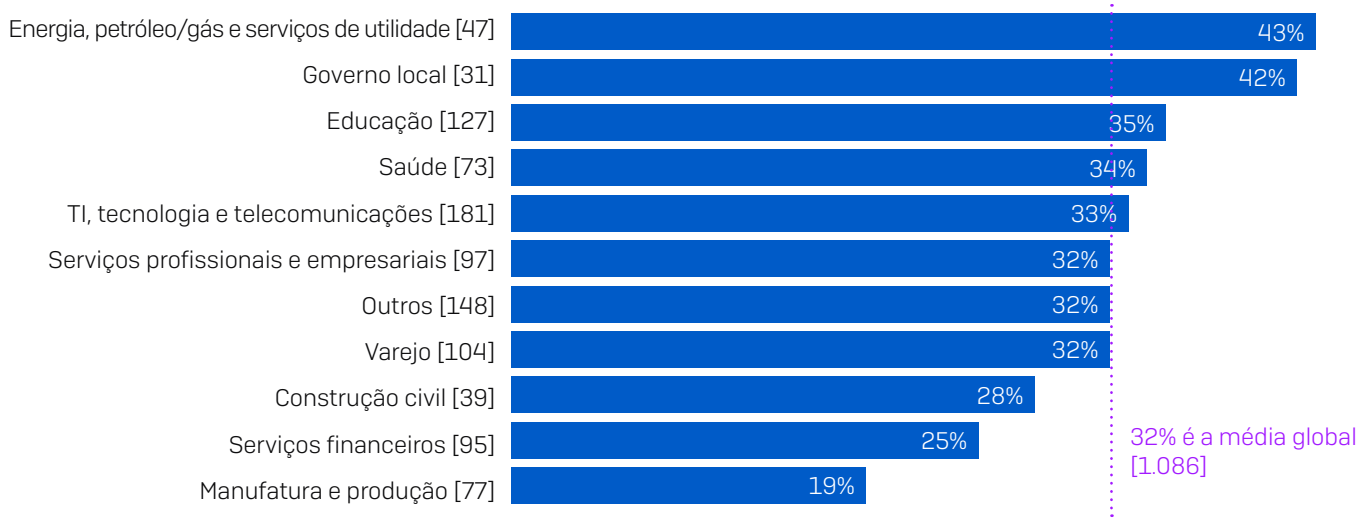
| 2020 | 2021 | |
|---|---|---|
| 26% | 32% | Pagaram resgate para reaver os dados |
| 56% | 57% | Usaram backups para reaver os dados |
| 12% | 8% | Usaram outros meios para reaver os dados |
| 94% | 96% | Total que conseguiu reaver os dados |

*Nota: Devido ao arredondamento, nem sempre os totais correspondem à soma dos valores separadamente*
*Sua organização conseguiu reaver os dados capturados no ataque de ransomware mais significativo?*
*[2021=1.086, 2020=1.849] organizações cujos dados foram criptografados*

Como se vê no gráfico acima, 32% pagaram o resgate para reaver seus dados, um aumento em relação aos 26% da pesquisa do ano anterior; 57% foram capazes de usar backups para restaurar seus dados, o que se equipara aos resultados obtidos no ano anterior. No geral, quase todos (96%) conseguiram reaver parte dos dados.

## Propensão de pagamento varia por setor

Existe uma considerável diferença quanto ao pagamento de regaste entre os setores.




*Sua organização conseguiu reaver os dados capturados no ataque de ransomware mais significativo? Sim, pagamos o resgate [números de base no gráfico] organizações em que os criminosos cibernéticos tiveram êxito na criptografia dos dados no ataque de ransomware mais significativo, omitindo algumas opções de resposta, dividido por setor*

**Energia, petróleo/gás e serviços de utilidade** é o setor mais propenso a pagar o resgate, com 43% dos respondentes das organizações aceitando a demanda de resgate. Esse setor normalmente tem um legado estrutural intenso que não pode ser facilmente atualizado, assim as vítimas se sentem coagidas a pagar o resgate para possibilitar a continuidade dos serviços.

**Governo local** registra o segundo mais alto índice de pagamentos de resgate (42%). É interessante notar que isso segue as descobertas recentes de que o governo local é o setor mais propenso a ter seus dados criptografados. Pode ser também que a propensão de as organizações de governo local pagarem leve os invasores a focar seus ataques mais complexos e eficazes nesse público.

Parece haver uma ligação entre a capacidade de uma organização restaurar seus dados a partir de backups e a probabilidade de ela pagar o resgate. **Manufatura e produção** é o setor com menor probabilidade de pagar resgate, além de ser o setor com maior habilidade para restaurar dados de backups (68%). Tal qual, a **construção civil**, bem como os **serviços financeiros** apresentam índices abaixo da média de pagamento de resgate e acima da média de habilidade de restaurar dados de backups.

**Governo central e NDPB** foi excluído deste gráfico porque apresenta uma base muito baixa de modo a oferecer significância estatística. Curiosamente, das 23 organizações nesse setor cujos dados foram criptografados, 61% relataram que foram capazes de restaurar os dados a partir de backups e apenas 26% pagaram o resgate. Isso é um indicativo que pode ajudar a explicar por que esse setor está particularmente sob a mira dos ataques estilo extorsão.

### Pagar o resgate recupera apenas parte dos seus dados

**65%**

**dos dados recuperados após pagamento do resgate**

*Quantidade média de dados que as organizações conseguiram reaver no ataque de ransomware mais significativo [344] organizações que pagaram o resgate para reaver seus dados*

O que os invasores deixam de dizer quando fazem suas demandas de regaste é que, mesmo que você pague, as chances de reaver todos os seus dados são ínfimas. Em média, as organizações que pagaram um resgate recuperaram apenas 65% de seus arquivos criptografados, ficando com mais de um terço de seus dados inacessíveis. Dos respondentes, 29% relataram que 50% ou menos de seus arquivos foram restaurados, e apenas 8% conseguiram reaver todos os dados.

## O custo do ransomware

### Pagamentos de resgate variam imensamente

Dos 357 respondentes que disseram que suas organizações pagaram o resgate, 282 também mencionaram a quantia exata que foi paga. Entre esse grupo, o **pagamento médio foi de US$ 170.404,00**. Contudo, o espectro de pagamentos de resgate foi bastante amplo. O pagamento mais comum foi US$ 10.000,00 (efetuado por 20 respondentes), e o pagamento mais alto foram exorbitantes US$ 3,2 milhões (efetuado por dois respondentes).

Esses números variam bastante dos valores em dólar de oito casas que dominaram as manchetes por diferentes motivos.

1. **Tamanho da organização.** Nossos respondentes são organizações de pequeno e médio porte, com entre 100 e 5.000 usuários que, em geral, têm menos recursos financeiros do que as empresas maiores. Os agentes de ransomware ajustam suas demandas de resgate de acordo com a capacidade de pagamento de suas vítimas, e normalmente aceitam pagamentos mais baixos das pequenas empresas. Os dados confirmam: a média de pagamento de resgate por organizações com 100 a 1.000 funcionários atingiu a marca de US$ 107.694,00, enquanto o resgate médio pago por organizações com 1.000 a 5.000 funcionários foi de US$ 225.588,00.
2. **Natureza do ataque.** Existem muitos agentes de ransomware e muitos tipos de ataque de ransomware, variando entre invasores mais bem equipados, que utilizam táticas, técnicas e procedimentos (TTPs) sofisticados que focam em alvos individuais, e operadores com poucas habilidades, que usam ransomwares "pré-prontos" e uma abordagem geral do tipo "spray and pray". Os invasores que investem pesado em um ataque direcionado buscarão altos resgates em pagamento por seus esforços, enquanto os operadores por trás dos ataques mais comuns geralmente aceitam menores retornos sobre seus investimentos (ROI).
3. **Localização.** Os invasores visam suas mais altas demandas de resgate às economias ocidentais desenvolvidas, motivados pelo entendimento de que podem pagar altas somas. Os dois resgates mais altos pagos foram relatados por respondentes na Itália.  Além disso, o pagamento médio de resgate entre os EUA, Canadá, Reino Unido, Alemanha e Austrália foi de US$ 214.096,00, valor 26% maior do que a média global (base: 101 respondentes). De modo recíproco, na Índia, o pagamento médio de resgate foi de US$ 76.619,00, menos da metade do número global (base: 86 respondentes).

## O custo de remediação de ransomware mais do que dobrou desde o ano passado

Pagar o resgate é apenas uma parte do custo de remediação de um ataque. Embora o número de ataques de ransomware e a porcentagem de ataques em que os adversários têm êxito na criptografia dos dados tenham caído desde o último ano, o custo geral de remediação de um ataque de ransomware subiu.

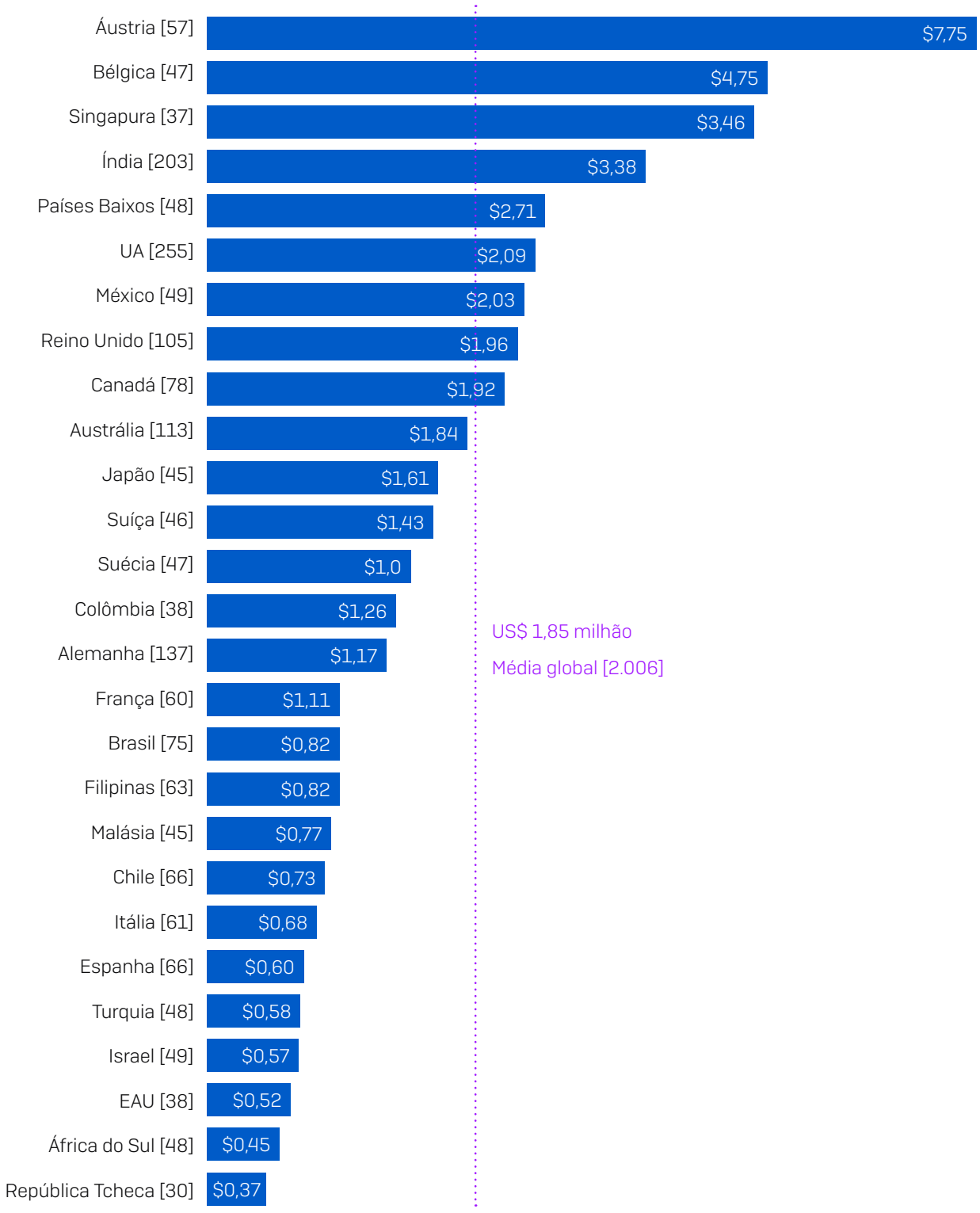
Os respondentes disseram que o custo médio para retificar o impacto do mais recente ataque de ransomware (considerando-se período de inatividade, tempo de pessoal, custo dos equipamentos, custo da rede, perda de oportunidades, resgate pago, etc.) foi US$ 1,85 milhão, mais do que o dobro do custo relatado no ano anterior de US$ 761.106,00.


*Média aproximada do custo para as organizações retificarem o impacto do mais recente ataque de ransomware (considerando-se período de inatividade, tempo de pessoal, custo dos equipamentos, custo da rede, perda de oportunidades, resgate pago, etc.) [2021=2.006, 2020=2.538] respondentes cuja organização foi atingida por ransomware no último ano, dividido por ano*

No último ano, os especialistas em ransomware da Sophos observaram um crescimento considerável em ataques de ransomware avançados combinando automação com hackers atuantes. Esses complexos ataques requerem complexos processos de recuperação, podendo este ser um fator elementar por trás do aumento geral nos custos de recuperação de ransomware.

## Custos de remediação variam baseados na sua localidade

Examinando os custos de remediação de ransomware no nível de país, observamos variações consideráveis.




*Média aproximada do custo para as organizações retificarem o impacto do mais recente ataque de ransomware [considerando-se período de inatividade, tempo de pessoal, custo dos equipamentos, custo da rede, perda de oportunidades, resgate pago, etc.] [números de base no gráfico] respondentes cuja organização foi atingida por ransomware no último ano, dividido por país, milhões de USD*

A Áustria se destaca como o país com o mais alto custo de remediação de ransomware. Houve vários ataques cibernéticos de alto escalão em organizações austríacas, com o ministério de exterior da Áustria declarando que foi alvo de um impostor e o grupo de ransomware Netwalker divulgando no Twitter ter roubado dados da cidade de Weiz, na Áustria. Vale notar que se excluirmos a Áustria dos dados, o custo médio de remediação cai para US$ 1,68 milhão, mais do que o dobro do valor do ano anterior.

Em geral, países com altos salários – Bélgica, Singapura, Países Baixos, Estados Unidos – relatam custos gerais entre os mais altos registrados, enquanto países com salários mais baixos – República Tcheca, África do Sul – relatam os custos gerais mais baixos. Isso reflete o esforço manual considerável necessário para remediar um ataque. De fato, o custo total para remediar um ataque de ransomware é 10 vezes a média de pagamento de resgate.

Israel está entre os países com os mais baixos custos gerais de remediação de ransomware, apesar de ter uma economia desenvolvida. Por questões geopolíticas, Israel é um grande alvo de ataques cibernéticos (não apenas ransomware), resultando em altíssimos níveis de expertise em defesa, preparo e remediação em todo o país. Esses se combinam de modo a diminuir o impacto financeiro de um ataque.

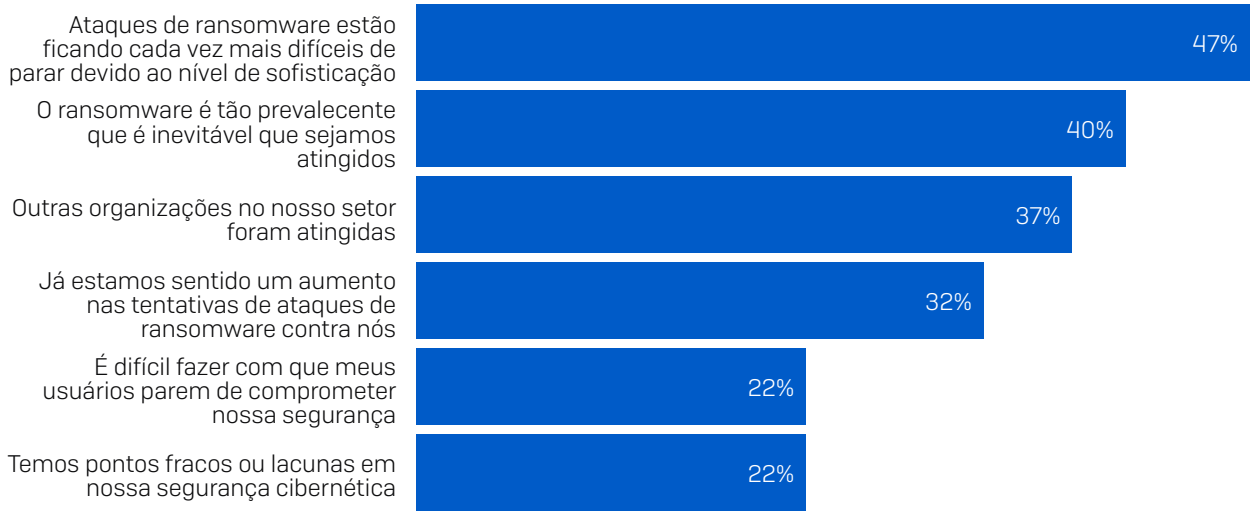
# O futuro

## Expectativas de ataques de ransomware variam

62% dos respondentes da pesquisa (3.353) relatam que suas organizações não foram atingidas por ransomware no último ano. Nesse grupo observamos variações consideráveis de atitude em relação ao tratamento e a confiança em lidar com o ransomware. 65% esperam ser atingidos por ransomware no futuro, enquanto 35% não esperando ser alvo de um ataque.

## Por que as organizações esperam ser atingidas por ransomware

Entre os 2.187 respondentes de organizações que não foram atingidas por ransomware no último ano, mas que esperam ser atingidas no futuro, o motivo mais comum de acharem que sofrerão um ataque é que "ataques de ransomware estão ficando cada vez mais difíceis de parar devido ao nível de sofisticação", citado por 47% dos respondentes neste grupo.



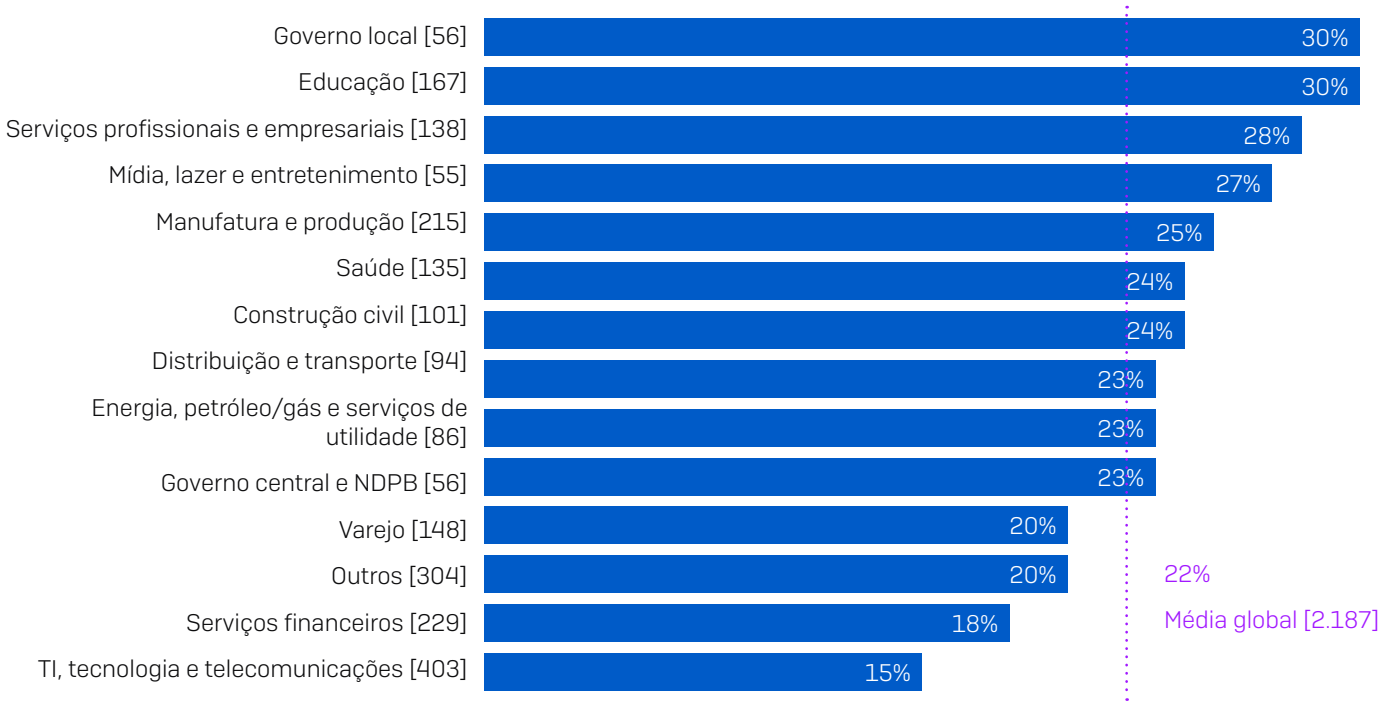

*Por que você espera que a sua organização seja atingida por ransomware no futuro? [2.187] organizações que não foram atingidas por ransomware no ano passado esperam ser atingidas no futuro, omitindo algumas opções de resposta*

Ainda que esse seja um número alto, o fato de que essas organizações estão atentas ao fato de o ransomware estar ficando cada vez mais avançado é algo bom e pode ter sido um fator contribuinte de terem sido capazes de bloquear possíveis ataques de ransomware no ano passado.

Dos respondentes, 22% consideram o comprometimento da segurança pelos usuários um fator principal quando se trata de ser atingido por ransomware no futuro. É animador notar que, em vista a invasores sofisticados, a maioria das equipes de TI não está mais saindo pela tangente e culpando seus usuários.

De modo similar, 22% dos respondentes admitem ter fraquezas ou lacunas na segurança cibernética. Ainda que claramente não seja uma boa ideia ter deficiências na segurança, reconhecê-las é um importante passo para fortalecer as suas defesas.

Aprofundando-se mais nesse ponto, vemos que os setores de governo local e educação são os mais propensos a admitir suas fraquezas em segurança (30% cada).




*Por que você espera que a sua organização seja atingida por ransomware no futuro? Temos pontos fracos ou lacunas em nossa segurança cibernética [números de base no gráfico] organizações que não foram atingidas por ransomware no ano passado esperam ser atingidas no futuro, omitindo algumas opções de resposta, dividido por setor*

Ainda que os respondentes a esta pergunta não tenham sido atingidos por ransomware no último ano, é provável que tenham sido influenciados pelas vastas experiências com ransomware em seus setores:

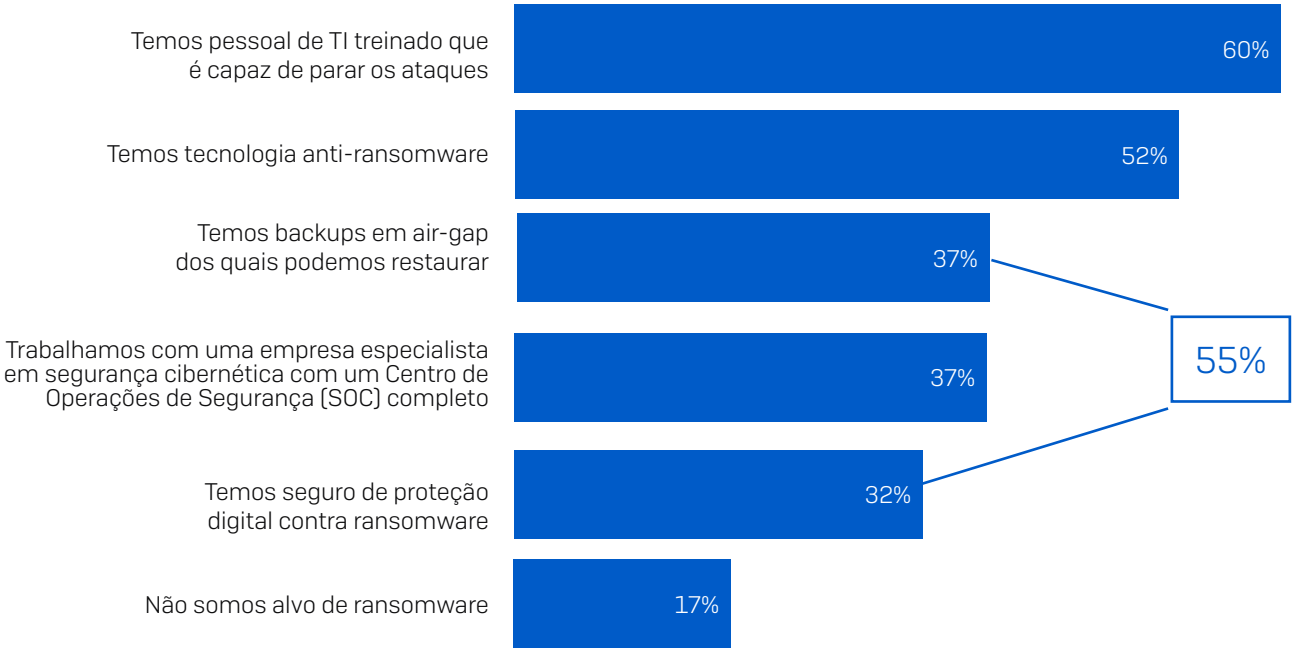
- O **governo local** é o setor em que os invasores têm maiores chances de obter êxito na criptografia dos dados da vítima
- **Educação** (juntamente com o varejo) é o setor que mostra a mais alta porcentagem de organizações atingidas por ransomware no último ano

Além disso, os dois setores normalmente têm dificuldade de obter fundos para recursos de tecnologia e TI, o que também leva a deficiências na segurança.

De modo recíproco, **IT, telecomunicações e tecnologia** (15%) e **serviços financeiros** (18%) têm a mais baixa porcentagem de respondentes que admitem lacunas de segurança. Esses setores são geralmente rápidos para adotar a nova tecnologia e têm orçamentos maiores, de modo a ter mais oportunidades para tratar de áreas com pontos fracos.

## Pessoal de TI treinado dá confiança ao ransomware

1.166 respondentes disseram não ter sido atingidos por ransomware no ano passado, e não esperam ser atingidos no futuro. O motivo nº 1 para essa confiança em face ao ransomware é ter pessoal de TI treinado capaz de interromper os ataques.




*Por que você não espera que a sua organização seja atingida por ransomware no futuro? [1.166] organizações que não foram atingidas por ransomware no ano passado e não esperam ser atingidas no futuro, omitindo algumas opções de resposta*

Enquanto as tecnologias avançadas e automatizadas são elementos essenciais de uma defesa anti-ransomware eficaz, interromper os invasores que trabalham ativamente também exige monitoramento e intervenção humana por profissionais capacitados. Seja seu pessoal interno ou profissionais contratados, os peritos humanos são únicos em sua capacidade de identificar alguns dos indicativos de que invasores de ransomware têm você na mira.

Dos respondentes, 37% deles que não esperam ser atingidos por ransomware trabalham com uma empresa especialista em segurança cibernética com um centro de operações de segurança (SOC). Apenas alguns anos atrás SOCs eram exclusividade das grandes empresas , portanto isso representa uma grande guinada na entrega de segurança cibernética para organizações de médio porte.

Mas não são só boas notícias. Alguns resultados são motivo de preocupação:

- 55% dos respondentes que não esperam ser atingidos estando acreditando em abordagens que não oferecem nenhuma proteção contra ransomware:
  - 37% dos respondentes mencionaram "backups air-gap" como o motivo de acharem que não serão atingidos. Backups, como vimos, são valiosas ferramentas para restaurar dados pós-ataque, mas eles não impedem que você seja atingido por um ataque.

- 32% dos respondentes dizem que ter seguro de proteção digital os protege contra ataques de ransomware. E, reenfatizando, o seguro pode ajudar a lidar com o problema após o ataque, mas não evita o ataque.

**N.B. Alguns respondentes selecionaram as duas opções, com 55% selecionando pelo menos uma dessas duas opções.**

- Além disso, 17% dos respondentes não acreditam ser alvo de ransomware. Mas isso não é verdade. Nenhuma organização está segura.

## Os planos de recuperação de incidente de malware são básicos

Responder a incidentes ou ataques cibernéticos críticos pode ser incrivelmente estressante. Enquanto nada pode aliviar por completo a tensão de encarar um ataque, ter um plano de resposta a incidentes eficiente em vigor é um modo infalível de minimizar o impacto.

Por isso é animador descobrir que 90% dos respondentes relatam que suas organizações têm uma plano de recuperação de incidente de malware, com um pouco mais da metade (51%) que afirmam ter um plano completo e detalhado, e 39% afirmam ter um plano parcialmente desenvolvido.

Há vários paralelos entre recuperar-se de um malware e recuperar-se de um desastre natural: nos dois cenários você precisa ser capaz de começar de novo, do zero. As Filipinas, que sofrem frequentes inundações e terremotos, é o país mais preparado para um incidente de malware, onde 83% dos respondentes têm planos de recuperação de incidentes de malware completos e detalhados.

## Organizações governamentais são as menos preparadas para responder a um ataque de malware

A maioria dos setores está bem-preparada para se recuperar de um incidente de malware. Contudo, as organizações governamentais despontaram como as menos preparadas: apenas 73% do **governo local** e 81% do **governo central e NDPB** têm um plano de recuperação de malware.

Isso é preocupante, pois esses setores estão entre os mais afetados por ransomware; o governo local é o setor mais propenso a ter seus dados criptografados em um ataque, enquanto o governo central e NDPB estão mais expostos à extorsão.

A falta de um plano de recuperação pode ser um fator contribuinte em colocar o governo local em segundo lugar na lista dos mais prováveis a pagar demandas de resgate.

# Recomendações

Com base nesses resultados, os especialistas da Sophos recomendam as seguintes práticas:

1. **Admita que você será atingido.** Ransomware continua a marcar forte presença. Não há setor, país ou organização de nenhum tamanho que esteja imune ao risco. É melhor se preparar e não ser atingido do que o contrário.

2. **Faça backups.** Backups são o método nº 1 utilizado pelas organizações para recuperar dados após um ataque. E como temos notado, mesmo que pague o resgate, você raramente irá reaver seus dados, ou seja, você terá que contar com backups de um jeito ou de outro.

3. **Implemente uma proteção em camadas.** Em face ao aumento considerável nos ataques de extorsão, manter os adversários fora do seu ambiente é o fator mais importante no momento. Use proteção em camadas para bloquear o máximo possível de pontos de ataque em todo o seu ambiente.

4. **Combine perícia humana e tecnologia anti-ransomware.** O fundamental para deter um ransomware é uma defesa profunda que combine tecnologia anti-ransomware dedicada e caça a ameaças conduzida por humano. A tecnologia oferece a escala e automação que você precisa, enquanto os peritos humanos são mais bem capacitados a detectar os indicativos de táticas, técnicas e procedimentos que um invasor habilidoso está tentando usar para entrar no seu ambiente. Se você não tem pessoal interno habilitado, pense sobre a possibilidade de contratar os serviços de uma empresa de segurança cibernética especializada – as SOCs agora são opções realistas para as organizações de todos os tamanhos.

5. **Não pague o resgate.** Sabemos que é fácil falar e mais difícil ainda fazer quando a sua organização se vê paralisada devido a um ataque de ransomware. Independentemente das considerações éticas, pagar o resgate é um modo ineficaz de reaver seus dados. Se decidir pagar, não deixe de incluir na sua análise de custos/benefícios a perspectiva de que seus adversários irão restaurar, em média, apenas dois terços dos seus arquivos.

6. **Tenha um plano de recuperação de malware.** A melhor forma de parar um ataque virtual antes que se torne uma violação total é se preparar com antecedência. As organizações que são vítimas de um ataque frequentemente se dão conta de que poderiam ter evitado boa parte do custo, estresse e interrupção se tivessem um plano de resposta a incidentes em vigor.

## Recursos extras

O Guia de Resposta a Incidentes da Sophos ajuda as organizações a definir a estrutura do seu plano de resposta a incidentes contra a segurança cibernética e explora as 10 etapas principais que o seu plano deve incluir.

O pessoal da defesa também achará útil as Quatro grandes dicas de peritos em resposta a incidentes, destacando os principais aprendizados que todos deveriam ter quando se trata de responder a incidentes de segurança cibernética.

Esses dois recursos se baseiam em experiências reais do mundo real das equipes da Sophos Managed Threat Response e Sophos Rapid Response, que coletivamente já responderam a milhares de incidentes de segurança cibernética.

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.



2021-04-19 (SB-NP)