SOPHOS

O CUSTO HUMANO DA VIGILÂNCIA: RESOLVENDO O ESGOTAMENTO DA SEGURANÇA CIBERNÉTICA EM 2025

Documento técnico Sophos. Agosto, 2025

Apresentação

A definição do cenário da segurança cibernética está cada vez mais atrelada à pressão implacável de ameaças cibernéticas sofisticadas, incluindo o ransomware. Este ambiente difuso de ameaças coloca grandes demandas nas equipes de TI e segurança cibernética, levando a um desafio significativo e crescente: a fatiga e o esgotamento da segurança cibernética.

Este relatório examina o impacto humano direto dessas pressões, levando a novos dados de pesquisa que revelam a predominância, os principais propulsores e as consequências do esgotamento, ressaltando como as soluções estratégicas podem mitigar essa questão crítica.

Os dados foram coletados em uma pesquisa desvinculada de fornecedores com 5.000 profissionais de TI e segurança cibernética em 17 países. A pesquisa foi realizada no primeiro trimestre de 2025 e os entrevistados basearam suas respostas em experiências vivenciadas nos últimos 12 meses antecedentes.

Entenda o que é fatiga e esgotamento de segurança cibernética

A **fatiga da segurança cibernética** se caracteriza[1] por um estado de exaustão mental e emocional, que se intensifica pelo constante estado de vigília, sobrecarga de alertas e a natureza de alto risco da defesa contra ameaças cibernéticas. Essa situação desencadeia uma experiência de drenagem emocional e cognitiva que os profissionais da área enfrentam.

O **esgotamento**, uma síndrome psicológica mais generalizada, engloba exaustão emocional, ceticismo e uma sensação de realização pessoal indistinta, muitas vezes resultante do estresse crônico no ambiente de trabalho. No espaço da segurança cibernética, a fatiga pode ser vista como uma manifestação direta ou um fator contribuinte significativo de um esgotamento nervoso maior.

O **esgotamento da segurança cibernética** é uma manifestação específica de uma teoria de esgotamento maior no contexto único e exclusivo da área da segurança cibernética. Ele engloba a exaustão mental, física e emocional causada pela exposição intensa e prolongada ao estresse inerente do trabalho em segurança cibernética.

Os profissionais que atuam nessa área encaram demandas emocionais e cognitivas únicas, incluindo o gerenciamento constante de alertas de segurança, que é imperativo para garantir a conformidade com regulamentos rigorosos, e a rapidez exigida na resposta às ameaças cibernéticas emergentes.

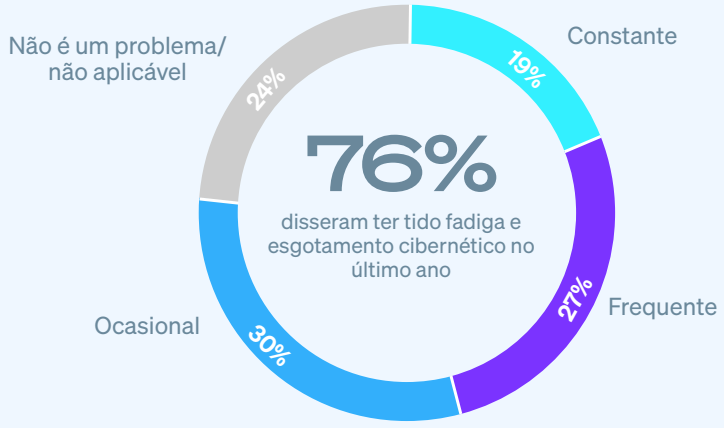
Essa exposição contínua à pressão de tarefas exigentes e a necessidade de respostas rápidas e precisas a incidentes são elementos fundamentais que aumentam o risco da fatiga e do esgotamento entre a força de trabalho da segurança cibernética.

Tensão persistente e extensas repercussões

A experiência do esgotamento

A pressão nos profissionais de segurança cibernética fica evidente quando observamos a amplitude das repercussões que as equipes de TI e segurança cibernética enfrentaram no decorrer do ano anterior.

Quando perguntados sobre experiências pessoais de fatiga cibernética ou esgotamento, 76% dos entrevistados afirmaram ter passado pela situação no último ano. Detalhando esses valores, observamos que 19% relataram isso como um problema “constante”, 27% o relatam como um problema “frequente” e 30% o relatam como um problema “ocasional”.



Você passou por alguma situação de fadiga ou esgotamento de segurança cibernética no último ano? n=5.000

Os dados revelaram que o esgotamento é uma questão persistente, independentemente do tamanho da organização: 76% dos entrevistados em empresas com 100 a 1.000 funcionários, 77% dos entrevistados em empresas com 1.001 a 3.000 funcionários e 75% dos entrevistados em empresas com 3.001 a 5.000 funcionários passaram por esgotamento nervoso.

E mais, o problema está piorando:
69% dos entrevistados disseram que a fatiga e o esgotamento da segurança cibernética aumentaram entre 2023 e 2024.

[1]Digital detox: exploring the impact of cybersecurity fatigue on employee productivity and mental health

As consequências do esgotamento

Não surpreende que o esgotamento nervoso cause impactos significativamente negativos nas pessoas que passam por ele, com quase metade (46%) relatando ansiedade elevada sobre ataques cibernéticos ou violações, quatro em cada dez (39%) admitindo queda de produtividade no trabalho e um terço (33%) dizendo-se desmotivado no trabalho.

Consequências da fatiga e do esgotamento de segurança cibernética

Impacto do esgotamento	Média (n=3.803)	Nível da experiência de esgotamento		
		Problema constante (n=944)	Problema frequente (n=1.357)	Problema ocasional (n=1.502)
Enfrentou ansiedade elevada sobre ataques cibernéticos e violações	**46%**	47%	45%	46%
Produtividade reduzida no trabalho	**39%**	36%	36%	43%
Motivação reduzida no trabalho	**33%**	34%	33%	34%
Precisou tirar folga no trabalho	**29%**	31%	28%	28%
Considerou mudar de carreira ou função	**23%**	29%	25%	17%
Considerou demitir-se do trabalho	**22%**	28%	25%	16%

Quais são as consequências pessoais da fatiga ou esgotamento cibernético? Entrevistados que disseram ter tido esgotamento nos últimos 12 meses. Números de base no gráfico.

Esses valores ressaltam um desafio cada vez mais presente e que enfraquece diretamente a eficiência e a sustentabilidade das defesas na segurança cibernética.

Causas básicas da pressão

A natureza exigente da defesa cibernética moderna, exacerbada pelo ritmo implacável de ataques cibernéticos, contribui significativamente para o esgotamento nervoso. Entre todos os entrevistados que disseram ter passado por uma experiência de fatiga cibernética ou esgotamento, as mudanças constantes em soluções e tecnologias de defesa cibernética foram o fator contribuinte mais comum (38%). Para aqueles que o esgotamento é um problema "constante", a natureza do trabalho de segurança cibernética, ou seja, tarefas rotineiras entremeadas a atividades direcionadas, é a causa mais comum, citada por 40% dos entrevistados.

Fatores que causam fatiga e esgotamento de segurança cibernética

Causa do esgotamento	Média (n=3.803)	Nível da experiência de esgotamento		
		Problema constante (n=944)	Problema frequente (n=1.357)	Problema ocasional (n=1.502)
Mudanças constantes em soluções e tecnologias de defesa cibernética	**38%**	36%	37%	41%
A natureza do trabalho de segurança cibernética (tarefas rotineiras entremeadas a atividades direcionadas)	**37%**	40%	36%	36%
Mudanças constantes em ameaças	**34%**	31%	31%	39%
A necessidade de cobertura 24/7	**32%**	30%	32%	33%
Pressão das mudanças em obrigações legais e regulatórias	**32%**	34%	34%	29%
Mudanças constantes em prioridades	**30%**	28%	29%	32%
Pressão da diretoria e/ou conselho executivo	**30%**	29%	30%	30%
Falta de pessoal treinado	**27%**	24%	26%	29%
Restrições no orçamento (excluindo funcionários)	**26%**	27%	28%	24%
Falta de acesso a suporte terceirizado especializado	**26%**	30%	25%	23%
Alto volume de alertas	**25%**	24%	26%	25%

Quais fatores foram a causa da fatiga ou esgotamento cibernético que você teve? Entrevistados que disseram ter tido esgotamento nos últimos 12 meses. Números de base no gráfico.

Em média, os entrevistados citaram três fatores separados que contribuíram para a situação de esgotamento que enfrentaram, destacando os vários pontos de pressão que as equipes de TI enfrentam.

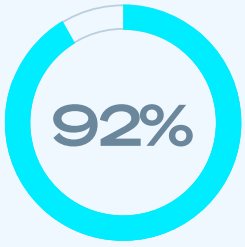
Impacto individual e organizacional

O esgotamento nervoso, quando não tratado, pode promover uma cascata de efeitos negativos que impactam tanto o bem-estar individual dos profissionais de segurança quanto a resiliência geral da organização.

- **Impacto individual:** os profissionais sofrem com o estresse elevado, ansiedade, insatisfação profissional e efeitos adversos à sua saúde física e mental. Isso pode também gerar tensões em relacionamentos pessoais e levar a um aumento na rotatividade.
- **Impacto organizacional:**
  - **Vulnerabilidade aumentada:** equipes exauridas estão mais propensas a erros e descuidos, levando a possíveis lacunas críticas de segurança e a um maior risco de violações bem-sucedidas.
  - **Eficiência reduzida:** o esgotamento afeta negativamente o foco, a tomada de decisão e a produtividade, comprometendo a capacidade de defesa da equipe contra ameaças avançadas.
  - **Atrito entre talentos:** o estresse elevado associado à função contribui para a rotatividade entre profissionais qualificados, exacerbando a escassez de talentos em segurança cibernética.
  - **Interrupção operacional:** uma postura de segurança comprometida devido ao esgotamento pode levar a incidentes de segurança mais frequentes e impactantes, incluindo ataques de ransomware, resultando em períodos de inatividade operacional e perdas financeiras significativas.

Medidas estratégicas e sua eficiência

As organizações estão empregando estratégias variadas para mitigar a fatiga da segurança cibernética. Ainda que medidas internas sejam benéficas, como fomentar uma cultura de apoio, oferecer recursos para uma boa saúde mental e investir no desenvolvimento profissional, a adoção de parcerias externas estratégicas, particularmente em serviços de detecção e resposta gerenciadas (MDR), se mostram bastante promissoras.



dos entrevistados impactados que usam MDR disseram que reduziu a fadiga e o esgotamento da segurança cibernética.

A pesquisa revela que os serviços MDR são uma forma altamente eficaz de aliviar o esgotamento nervoso, com 92% dos entrevistados afetados que usaram um serviço dizendo que isso reduziu a fatiga e o esgotamento da segurança cibernética. Entre aqueles que veem o problema como "constante", metade deles relatou uma redução "significativa" e 45% disseram que o serviço reduziu o esgotamento "relativamente". Isso indica um alto consenso de que transferir a carga de operações críticas de segurança para provedores especializados em MDR reduz substancialmente a pressão sobre as equipes internas.

Eficácia dos serviços MDR em reduzir a fadiga e o esgotamento da segurança cibernética

Impacto	Média (n=3.750)	Nível da experiência de esgotamento		
		Problema constante (n=940)	Problema frequente (n=1.340)	Problema ocasional (n=1.470)
Reduziu o esgotamento significativamente	**39%**	50%	35%	34%
Reduziu o esgotamento relativamente	**53%**	45%	56%	56%
Total	**92%**	95%	92%	90%

Se a sua organização usa um serviço de detecção e resposta gerenciadas (MDR), isso ajudou a diminuir os casos de fatiga e esgotamento da segurança cibernética? Entrevistados que disseram ter tido esgotamento nos últimos 12 meses e cujas organizações usam um serviço MDR. Números de base no gráfico.

Sophos MDR como pilar de uma defesa sustentável

A luta contra o crime cibernético é implacável. Para construir uma defesa realmente resiliente, as organizações devem não apenas enriquecer sua capacidade tecnológica, mas também salvaguardar o bem-estar da sua defesa humana.

O Sophos MDR oferece uma poderosa solução para aliviar o esgotamento da segurança cibernética ao tratar de várias das causas fundamentais:

- **Aprendizado constante:** a equipe do Sophos MDR está profundamente sintonizada a inovações em tecnologias de defesa cibernética e ameaças, assegurando que os clientes desfrutem todos os benefícios dos desenvolvimentos tecnológicos para otimizar suas defesas.
- **Monitoramento contínuo e resposta imediata a ataques:** analistas especializados do Sophos MDR cuidam da natureza imprevisível das operações de segurança para os clientes. Desde tarefas como monitoramento contínuo, detecção e investigação, que consomem largura de banda significativa, até a resposta a ameaças em grande escala na eventualidade de um incidente, que põe fim à luta que as equipes internas enfrentam (geralmente fora do horário comercial).
- **Acesso direto a especialistas em segurança:** os clientes Sophos MDR podem trabalhar com a expertise de centenas de analistas em todas as áreas de operações de segurança, incluindo especialistas em caça a ameaças, detecção, investigação e resposta, e peritos e agentes de ameaças e malwares que trabalham nos bastidores.
- **Cobertura 24/7:** sete centros globais de operações de segurança oferecem cobertura, assegurando que os clientes estejam totalmente protegidos a qualquer hora do dia e da noite.
- **Triagem de alertas alimentada por IA:** o grande volume de alertas pode ser tornar excessivo facilmente. O Sophos MDR combina ferramentas de triagem alimentadas por IA com uma profunda perícia humana para que possamos identificar rapidamente as atividades suspeitas em meio à balbúrdia.

Ao estabelecer uma parceria com o Sophos MDR, as organizações podem assumir uma postura de segurança robusta e proativa que não apenas fortalece suas defesas contra ameaças como ransomware, mas também apoia o bem-estar mental de seus profissionais de segurança cibernética, assegurando uma defesa humana eficiente e sustentável em face da evolução das ameaças cibernéticas.

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

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.

2025-08-26 WP (MP)

SOPHOS