**Relatório da Fortinet indica que responsabilidade de cibersegurança em OT está a aumentar dentro dos níveis de liderança executiva**

*Mais de metade (52%) das organizações afirmam que os CISO/CSO são responsáveis pela OT, em comparação com os 16% registados em 2022, no entanto a maioria (95%) das organizações refere que a OT é da responsabilidade das funções C-suite acima dos* *43% em 2022.*

**Lisboa, Portugal – 22 de julho de 2025**

**Resumo**

A [Fortinet](https://www.fortinet.com/?utm_source=website&utm_medium=pr&utm_campaign=fortinet), líder mundial de cibersegurança que fomenta a convergência entre segurança e redes, apresentou os resultados do seu relatório global [2025 State of Operational Technology and Cybersecurity Report](https://www.fortinet.com/resources/reports/state-ot-cybersecurity). Os recentes dados representam o estado atual da cibersegurança da tecnologia operacional (OT) e destacam as oportunidades de melhoria contínua para as organizações protegerem um cenário de ameaças de IT/OT em constante expansão. Para além das tendências e conhecimentos que afetam as organizações de OT, o relatório oferece um conjunto de melhores práticas para ajudar as equipas de segurança de TI e OT a proteger melhor os seus ambientes.

"*A sétima edição do State of Operational Technology and Cybersecurity Report da Fortinet mostra que as organizações estão a levar a segurança de OT mais a sério. Vemos esta tendência refletida num aumento considerável na atribuição de responsabilidade pelo risco de OT ao C-suite, juntamente com um aumento nas organizações que relatam taxas crescentes de maturidade da segurança de OT*", afirma **Nirav Shah, Senior Vice President, Products and Solutions, at Fortinet.** "*Juntamente com estas tendências, estamos a assistir a uma diminuição no impacto das invasões em organizações que priorizam a segurança de OT. Todos, desde a direção até às equipas de gestão, precisam de estar comprometidos com a proteção de sistemas de OT sensíveis e alocar os recursos necessários para proteger as suas operações críticas."*

As principais conclusões do inquérito global incluem:

### **Responsabilidade pela segurança da OT continua a aumentar nos níveis executivos:** Tem existido um aumento significativo na tendência global das empresas que planeiam integrar a cibersegurança sob a alçada do CISO ou de outros executivos. À medida que a responsabilidade continua a ser transferida para as lideranças executivas, a segurança da OT é elevada para o nível superior do board. Os principais líderes internos que influenciam as decisões de cibersegurança das OT têm neste momento maior probabilidade de ser o CISO ou o CSO, por uma margem cada vez maior. Agora mais da metade (52%) das organizações referem que o CISO/CSO é o responsável pela OT, contra 16% verificados em 2022. Para todas as funções de C-suite, este valor aumentou para os 95%. Além disso, o número de organizações que pretendem transferir a cibersegurança de OT sob o CISO nos próximos 12 meses aumentou de 60% para 80% em 2025.

### **A maturidade de cibersegurança das OT está a afetar o impacto das intrusões:** A maturidade da segurança OT autodeclarada registou um progresso notável este ano. No nível 1 básico, 26% das organizações relatam ter estabelecido visibilidade e implementado segmentação, em comparação com 20% no ano anterior. O número superior de organizações afirmou que a sua maturidade de segurança encontra-se na fase de acesso e definição de perfis do Nível 2. O relatório também encontrou uma correlação entre maturidade e ataques. As organizações que afirmaram ser mais maduras (mais elevadas nos níveis 0-4) estão a sofrer menos ataques ou indicam que são mais capazes de lidar com táticas de menor sofisticação, como o *phishing.* É importante notar que algumas táticas, como as ameaças persistentes avançadas (APT) e o malware OT, são difíceis de detetar e as organizações menos maduras podem não ter as soluções de segurança necessárias para determinar a sua existência. Em termos gerais, embora quase metade das organizações tenha sofrido **impactos,** estes **estão a diminuir**, com uma redução notável nas interrupções operacionais que **afetaram as receitas, que caíram de 52% para 42%.**

### **Adoção das melhores práticas de cibersegurança está a ter um impacto positivo:** Para além dos níveis de maturidade afetar o impacto das intrusões, tudo aponta para que a adoção de melhores práticas, como a implementação de uma higiene cibernética básica e uma melhor formação e sensibilização, está a ter um impacto real, incluindo uma queda significativa no comprometimento do correio eletrónico empresarial. Outras práticas recomendadas incluem a incorporação de inteligência contra ameaças, que aumentou (49%) desde 2024. Além disso, o relatório observou uma diminuição significativa no número de fornecedores de dispositivos OT, o que é um sinal de maturidade e eficiência operacional. Mais organizações (78%) estão agora a utilizar apenas um a quatro fornecedores de OT, o que indica que muitas destas organizações estão a consolidar fornecedores como parte das suas melhores práticas. A consolidação de fornecedores de cibersegurança também é um sinal de maturidade e corresponde às experiências dos clientes da Fortinet com a Fortinet OT Security Platform. A rede unificada e a segurança em locais remotos de OT aumentaram a visibilidade e reduziram as ciberameaças, levando a uma redução de 93% nos incidentes cibernéticos em comparação com uma rede plana. As soluções simplificadas da Fortinet também levaram a uma melhoria de 7x em termos de desempenho através de reduções na triagem e na sua configuração. 1

**Boas Práticas**

O **Relatório Global 2025 State of Operational Technology and Cybersecurity** da Fortinet fornece informações acionáveis para que as organizações reforcem a sua postura de segurança. As organizações podem enfrentar os desafios de segurança em OT adotando as seguintes boas práticas:

* **Estabelecer visibilidade e controlos compensatórios para os ativos OT**:As organizações precisam de ter a capacidade de ver e compreender tudo o que está nas suas redes OT. Depois de estabelecida a visibilidade, devem proteger os dispositivos críticos e aqueles que possam ser vulneráveis, o que exige controlos compensatórios de proteção especificamente concebidos para dispositivos OT sensíveis. Capacidades como políticas de rede com reconhecimento de protocolos, análise da interação entre sistemas e monitorização de endpoints podem detetar e prevenir o comprometimento de ativos vulneráveis.
* **Implementar segmentação**: Reduzir as intrusões requer um ambiente OT reforçado, com controlos rigorosos de política de rede em todos os pontos de acesso. Esta arquitetura de defesa de OT começa com a criação de zonas ou segmentos de rede. Normas como a ISA/IEC 62443 preconizam explicitamente a segmentação para impor controlos entre as redes OT e IT e entre sistemas OT. As equipas devem também avaliar a complexidade global da gestão da solução e considerar os benefícios de uma abordagem integrada ou baseada em plataforma, com capacidades de gestão centralizada.
* **Integrar OT nas operações de segurança (SecOps) e no planeamento da resposta a incidentes**: As organizações devem evoluir no sentido de operações de segurança conjuntas IT/OT (SecOps). Para tal, a OT tem de ter uma consideração específica nos planos de SecOps e resposta a incidentes, em grande parte devido às diferenças entre ambientes OT e IT, desde os tipos de dispositivos únicos até às consequências mais amplas de uma violação OT afetar operações críticas. Um passo essencial nesta direção é a inclusão do ambiente OT da organização nos playbooks. Esta preparação avançada promoverá uma melhor colaboração entre as equipas de IT, OT e produção, permitindo avaliar adequadamente os riscos cibernéticos e de produção. Pode também significar para o CISO ter a consciência, a priorização, o orçamento e os recursos humanos adequados.
* **Considerar uma abordagem baseada em plataforma para a arquitetura global de segurança**: Para fazer face às ameaças OT em rápida evolução e a uma superfície de ataque em expansão, muitas organizações reuniram um conjunto alargado de soluções de segurança de diferentes fornecedores. Isto resultou numa arquitetura de segurança excessivamente complexa, que dificulta a visibilidade e aumenta a sobrecarga dos recursos limitados das equipas de segurança. Uma abordagem baseada em plataforma pode ajudar as organizações a consolidar fornecedores e simplificar a sua arquitetura. Uma plataforma de segurança robusta, com capacidades específicas para redes IT e ambientes OT, pode proporcionar uma integração de soluções que melhora a eficácia da segurança e permite uma gestão centralizada para maior eficiência. A integração pode ainda proporcionar uma base para respostas automatizadas a ameaças.
* **Adotar inteligência de ameaças e serviços de segurança específicos para OT**: A segurança OT depende da consciencialização atempada e de análises precisas sobre riscos iminentes. Uma arquitetura de segurança baseada em plataforma deve também aplicar inteligência de ameaças alimentada por IA, para proteção quase em tempo real contra as ameaças mais recentes, variantes de ataques e vulnerabilidades. As organizações devem garantir que as suas fontes de inteligência de ameaças e conteúdos incluem informações robustas e específicas de OT nos seus feeds e serviços.

**Overview do Relatório**

* O Relatório Fortinet 2025 sobre o Estado da Tecnologia Operacional e da Cibersegurança baseia-se em dados de um inquérito global realizado a mais de 550 profissionais de OT, conduzido por uma empresa de pesquisa independente.
* Os inquiridos pertencem a diversas regiões do mundo, incluindo Austrália, Nova Zelândia, Argentina, Brasil, Canadá, China Continental, Colômbia, Dinamarca, Egito, França, Alemanha, Hong Kong, Índia, Indonésia, Israel, Itália, Japão, Malásia, México, Noruega, Filipinas, Polónia, Portugal, Singapura, África do Sul, Coreia do Sul, Espanha, Taiwan, Tailândia, Reino Unido e Estados Unidos, entre outros.
* Os participantes representam uma variedade de indústrias com forte utilização de OT, incluindo: indústria transformadora, transporte/logística, saúde/farmacêutica, petróleo, gás e refinaria, energia/utilities, química/petroquímica e água/águas residuais.
* A maioria dos inquiridos, independentemente do cargo, está profundamente envolvido nas decisões de compra de cibersegurança. Muitos são responsáveis pela tecnologia operacional nas suas organizações e/ou têm responsabilidade direta pela produção ou operações industriais.

**Recursos Adicionais**

* Aceda ao [relatório completo](https://www.fortinet.com/resources/reports/state-ot-cybersecurity) para saber mais sobre o Estado da Segurança em OT em 2025.
* Descubra as [Solucões de Segurança de OT](https://www.fortinet.com/solutions/ot-security) da Fortinet.
* [Participe no webinar](https://events.fortinet.com/otwebinars2025/analyzingtrends) agendado para o dia 7 de Agosto para receber mais insights sobre o relatório
* Saiba mais sobre o [compromisso da Fortinet](https://trust.fortinet.com/?itemName=infrastructure&source=click) com a segurança e integridade do produto, e leia este [post recente no blog](https://www.fortinet.com/blog/psirt-blogs/proactive-responsible-disclosure-is-one-cucial-way-fortinet-strengthens-customer-security) sobre este compromisso de longa data com o desenvolvimento responsável do produto e abordagem de divulgação de vulnerabilidades e políticas.
* Read about how [Fortinet customers](https://www.fortinet.com/customers?utm_source=website&utm_medium=pr&utm_campaign=customers) are securing their organizations.
* Follow Fortinet on [X](https://twitter.com/Fortinet), [LinkedIn](https://www.linkedin.com/company/fortinet/), [Facebook](https://www.facebook.com/Fortinet/), and [Instagram](https://www.instagram.com/fortinet/). Subscribe to Fortinet on our [blog](https://www.fortinet.com/blog?utm_source=website&utm_medium=pr&utm_campaign=blog) or [YouTube](https://www.youtube.com/channel/UCJHo4AuVomwMRzgkA5DQEOA).

**Sobre a Fortinet**

A [Fortinet](https://www.fortinet.com/blog?utm_source=pr&utm_medium=pr&utm_campaign=boiler%22%20\t%20%22_blank) é uma força motriz na evolução da cibersegurança e na convergência da rede com a segurança. A sua missão é proteger pessoas, dispositivos e dados em qualquer lugar, sendo que hoje oferece cibersegurança onde for necessário, com um portfólio com mais de 50 produtos de nível empresarial. Mais de meio milhão de clientes confiam nas soluções Fortinet, que se encontram entre as mais adotadas, mais patenteadas e mais validadas na indústria. O [Fortinet Training Institute](https://www.fortinet.com/nse-training?utm_source=pr&utm_campaign=nse-training%22%20\t%20%22_blank), um dos maiores e mais amplos programas de formação da indústria, dedica-se a tornar a formação em cibersegurança e novas oportunidades de carreira disponíveis a todos. A colaboração com organizações de alto nível e respeitadas dos sectores público e privado, incluindo CERTs, entidades governamentais e académicas, é um aspeto fundamental do compromisso da Fortinet para melhorar a ciber resiliência a nível global. A [FortiGuard Labs](https://www.fortinet.com/fortiguard/labs?utm_source=pr&utm_campaign=fortiguardlabs%22%20\t%20%22_blank), a organização de elite de investigação e inteligência sobre ameaças da Fortinet, desenvolve e utiliza tecnologias inovadoras como *Machine Learning* e *AI* para fornecer atempadamente aos clientes a melhor proteção de forma consistente e medidas de ação inteligentes na contenção de ameaças. Saiba mais em  [https://www.fortinet.com](https://www.fortinet.com/%22%20/t%20%22_blank), no [Blog da Fortinet](https://www.fortinet.com/blog?utm_source=blog&utm_medium=blog&utm_campaign=blog%22%20\t%20%22_blank), e na [FortiGuard Labs](https://www.fortinet.com/fortiguard/labs?utm_source=pr&utm_medium=pr&utm_campaign=fglabs%22%20\t%20%22_blank).