**Falta de competências em cibersegurança contribuiu para 80% das tentativas de ataques, segundo o novo relatório da Fortinet**

* 89% das empresas globais têm objetivos explícitos de diversidade, na contratação
* 75% das organizações têm estruturas formais para recrutar especificamente mais mulheres
* 59% têm estratégias em vigor para contratar minorias.

**Lisboa, Portugal – 03 de Maio 2022**

**Sandra Wheatley, SVP Marketing, Threat Intelligence e Influencer Communications da Fortinet**

"De acordo com o relatório da Fortinet, a falta de competências não é apenas um desafio de escassez de talento, mas tem também um impacto severo nos negócios, tornando-o numa das principais preocupações dos líderes executivos em todo o mundo. Através dos programas da Fortinet Training Advancement Agenda (TAA) e do Training Institute, estamos empenhados em enfrentar os desafios revelados no relatório através de várias iniciativas, incluindo programas focados em certificações de cibersegurança e no recrutamento de mais mulheres para a cibersegurança. Como parte deste compromisso, a Fortinet comprometeu-se a formar um milhão de profissionais para aumentar as competências cibernéticas, a consciencialização e a fazer a diferença no gap de competências até 2026".

A [Fortinet](https://www.fortinet.com/?utm_source=pr&utm_campaign=fortinet)®, líder mundial em soluções amplas, integradas e automatizadas de cibersegurança, acaba de divulgar o seu [relatório Cybersecurity Skills Gap 2022](https://www.fortinet.com/content/dam/fortinet/assets/reports/report-2022-skills-gap-survey.pdf?utm_source=pr&utm_campaign=report-2022-skills-gap-survey). O novo relatório global revela que a escassez de competências cibernéticas continua a ter múltiplos desafios e repercussões para as organizações, incluindo a ocorrência de violações de segurança e, consequentemente, perda de dinheiro. Como resultado, o [gap de competências](https://www.fortinet.com/training/taa?utm_source=pr&utm_campaign=taa) continua a ser uma das principais preocupações dos executivos de nível C e está a tornar-se cada vez mais uma prioridade a nível de direção. O relatório também sugere formas de abordar o gap de competências, tais como através de [formações e certificações](https://www.fortinet.com/nse-training?utm_source=pr&utm_campaign=nse-training) para aumentar o conhecimento dos colaboradores.

**O impacto global generalizado da escassez de competências cibernéticas**

De acordo com o [relatório Cyber Workforce](https://www.isc2.org/News-and-Events/Press-Room/Posts/2021/10/26/ISC2-Cybersecurity-Workforce-Study-Sheds-New-Light-on-Global-Talent-Demand) (ISC)2 de 2021, e a nível global, o número de profissionais dedicados à Cibersegurança, precisa de aumentar 65% para defender eficazmente os ativos críticos das organizações. Embora o número de profissionais necessários para preencher a lacuna tenha diminuído de 3,12 milhões para 2,72 milhões no ano passado, esta é ainda uma lacuna significativa que deixa as organizações vulneráveis.

O [relatório](https://www.fortinet.com/content/dam/fortinet/assets/reports/report-2022-skills-gap-survey.pdf?utm_source=pr&utm_campaign=report-2022-skills-gap-survey) da Fortinet demonstra múltiplos riscos resultantes do gap de competências cibernéticas. Mais, em particular, 8 em cada 10 das organizações inquiridas sofreram pelo menos um ataque que poderiam atribuir à falta de competências ou de sensibilização no que diz respeito à cibersegurança. O inquérito também mostrou que, globalmente, 64% das organizações sofreram violações que resultaram em perda de receitas, custos de recuperação e/ou multas.

Tendo em conta os custos crescentes dos ataques nos lucros e na reputação das organizações, a cibersegurança está a tornar-se cada vez mais uma prioridade ao nível da administração. Globalmente, 88% das organizações, que têm um conselho de administração, informaram que o seu conselho faz perguntas específicas sobre cibersegurança e 76% das organizações têm um conselho de administração que recomendou um aumento no número de especialistas em TI e cibersegurança.

**Avanço das Competências de Cibersegurança através de Formações e Certificações**

O [relatório da Fortinet sobre o gap de competências](https://www.fortinet.com/content/dam/fortinet/assets/reports/report-2022-skills-gap-survey.pdf?utm_source=pr&utm_campaign=report-2022-skills-gap-survey) demonstrou que as [formações e as certificações](https://www.fortinet.com/nse-training?utm_source=pr&utm_campaign=nse-training) são formas críticas de as organizações resolverem ainda mais o gap de competências. O relatório revelou que 95% dos líderes acredita que as certificações focadas na tecnologia têm um impacto positivo no seu papel e na sua equipa, enquanto 81% dos líderes prefere contratar pessoas com certificações. Além disso, 91% dos inquiridos partilhou que está disposto a pagar a um colaborador para obter cibercertificações. Uma das principais razões para as [certificações](https://training.fortinet.com/local/staticpage/view.php?page=certifications&utm_source=pr&utm_campaign=q2-nse) serem altamente consideradas deve-se à sua validação do aumento do conhecimento e consciencialização sobre cibersegurança.



Além da valorização das certificações, 87% das organizações implementaram um programa de formação para aumentar a consciência cibernética. No entanto, 52% dos líderes acredita que os seus colaboradores ainda carecem dos conhecimentos necessários, o que levanta questões sobre a eficácia dos seus atuais programas de sensibilização para a segurança.

Para as organizações que procuram formação de sensibilização sobre segurança, a Fortinet oferece um [serviço Security Awareness and Training](https://www.fortinet.com/training/security-awareness-training?utm_source=pr&utm_campaign=security-awareness-training) através do premiado Fortinet Training Institute. O serviço protege ainda mais os bens digitais críticos das organizações contra ameaças cibernéticas, através da sensibilização dos colaboradores para a cibersegurança. Este serviço recebe atualizações do [FortiGuard Labs](https://www.fortinet.com/fortiguard/labs?utm_source=pr&utm_campaign=fortiguardlabs) da Fortinet para que os colaboradores aprendam e se mantenham a par dos mais recentes métodos de ciberataque em evolução, para impedir a introdução de violações e riscos na empresa.

**Enfrentar os desafios do recrutamento e da retenção com compromissos de diversidade**

Um desafio significativo para as organizações tem sido encontrar e manter as pessoas certas para preencher funções críticas de segurança, desde especialistas em segurança na cloud a analistas de SOC. O [relatório](https://www.fortinet.com/content/dam/fortinet/assets/reports/report-2022-skills-gap-survey.pdf?utm_source=pr&utm_campaign=report-2022-skills-gap-survey) concluiu que 60% dos líderes admite que a sua organização luta com o recrutamento e 52% luta para reter talentos.

Entre os desafios de contratação está o recrutamento de mulheres, universitários licenciados e minorias. Globalmente, 7 em cada 10 líderes veem o recrutamento de mulheres e novos licenciados como um obstáculo de topo na contratação e 61% dizem que a contratação de minorias tem sido um desafio. À medida que as organizações procuram formar equipas mais capazes e mais diversificadas, 89% das empresas globais têm objetivos explícitos de diversidade como parte da sua estratégia de contratação, de acordo com o relatório. O relatório também demonstrou que 75% das organizações têm estruturas formais para recrutar especificamente mais mulheres e 59% têm estratégias em vigor para contratar minorias. Além disso, 51% das organizações têm feito esforços para contratar mais veteranos.

**Sobre o Cybersecurity Skills Gap 2022 da Fortinet:**

* O inquérito foi realizado entre mais de 1200 decisores de TI e de cibersegurança de 29 locais diferentes, incluindo os EUA, França, Japão, México, entre outros.
* Os inquiridos correspondem a diversas indústrias, incluindo tecnologia (28%), produção (12%) e serviços financeiros (10%).

**Recursos adicionais**

* Consulte o nosso [blog](https://www.fortinet.com/blog/industry-trends/global-cybersecurity-skills-gap-report-findings) para mais informações sobre o relatório Cybersecurity Skills Gap 2022.
* Saiba mais sobre a [formação gratuita de cibersegurança da Fortinet](https://www.fortinet.com/training/cybersecurity-professionals?utm_source=blog&utm_campaign=freetraining), que inclui uma ampla consciencialização cibernética e formação de produtos. Como parte da Training Advancement Agenda (TAA), da Fortinet, o Fortinet Training Institute também oferece formação e certificação através dos programas [Network Security Expert (NSE)](https://www.fortinet.com/training-certification?utm_source=blog&utm_campaign=cert), [Academic Partner](https://www.fortinet.com/training/security-academy-program?utm_source=blog&utm_campaign=academy) e [Education Outreach](https://www.fortinet.com/training/education-outreach-program?utm_source=blog&utm_campaign=education).
* [Veja](https://youtu.be/C5PuGKKNzpU) como a Fortinet torna possível a existência de um mundo digital em que possa sempre confiar e [veja](https://www.youtube.com/watch?v=x8US5w7D5Mc) como a plataforma [Fortinet Security Fabric](https://www.fortinet.com/solutions/enterprise-midsize-business/security-fabric.html?utm_source=pr&utm_campaign=security-fabric) oferece proteção ampla, integrada e automatizada em toda a infraestrutura digital de uma organização.
* Leia mais sobre como os [clientes da Fortinet](https://www.fortinet.com/customers.html?utm_source=pr&utm_campaign=customers) estão a proteger as suas organizações.
* Saiba mais sobre as Inteligência de Ameaças e investigação do [FortiGuard Labs](https://www.fortinet.com/fortiguard/labs?utm_source=pr&utm_campaign=FortiGuardLabs) ou os [Alertas de Outbreak](https://www.fortinet.com/fortiguard/outbreak-alert), que fornecem medidas para mitigar ataques de cibersegurança.
* Saiba mais sobre o [portfólio](https://www.fortinet.com/fortiguard/labs?tab=security-subscriptions) de serviços de segurança FortiGuard da Fortinet.
* Participe na [Fortinet User Community (Fuse)](https://fusecommunity.fortinet.com/home?utm_source=pr&utm_campaign=fuse-community). Partilhe ideias e comentários, saiba mais sobre os nossos produtos e tecnologia e conecte-se com colegas.
* Siga a Fortinet no [Twitter](https://twitter.com/Fortinet), [LinkedIn](https://www.linkedin.com/company/fortinet), [Facebook](https://www.facebook.com/fortinet/) e [Instagram](https://www.instagram.com/behindthefirewall/). Subscreva a Fortinet no [YouTube](https://www.youtube.com/channel/UCJHo4AuVomwMRzgkA5DQEOA?sub_confirmation=1).

**Sobre a Fortinet**

A Fortinet (NASDAQ: FTNT) torna possível a existência de um mundo digital em que podemos sempre confiar através da sua missão de proteger pessoas, dispositivos e dados em qualquer lugar. É por isso que as maiores empresas, fornecedores de serviços, e organizações governamentais, a nível mundial, escolhem a Fortinet para acelerar, com segurança, a sua jornada digital. A plataforma Fortinet Security Fabric oferece proteções amplas, integradas e automatizadas em toda a superfície de ataque digital, protegendo dispositivos, dados, aplicações e ligações críticas desde o data center até à cloud e ao escritório em casa. Ocupando a liderança do mercado de cibersegurança, com o maior número de dispositivos de segurança vendidos em todo o mundo, mais de 565.000 clientes confiam na Fortinet para proteger os seus negócios. Além disso, o Fortinet NSE Training Institute, uma iniciativa do Training Advancement Agenda (TAA) da Fortinet, oferece um dos maiores e mais abrangentes programas de formação do setor, com o objetivo de viabilizar a capacitação em segurança cibernética e gerar novas oportunidades de carreira para todos. Saiba mais em <https://www.fortinet.com> , no [Fortinet Blog](https://www.fortinet.com/blog?utm_source=pr&utm_campaign=blog), ou [FortiGuard Labs](https://www.fortinet.com/fortiguard/labs?utm_source=pr&utm_campaign=FortiGuardLabs).

*Copyright © 2022 Fortinet, Inc. Todos os direitos reservados. Os símbolos ® e ™ denotam respetivamente marcas comerciais registadas a nível federal e marcas comerciais de direito comum da Fortinet, Inc., suas subsidiárias e afiliadas. As marcas comerciais da Fortinet incluem, mas não estão limitadas ao seguinte: Fortinet, o logo da Fortinet, FortiGate, FortiOS, FortiGuard, FortiCare, FortiAnalyzer, FortiManager, FortiASIC, FortiClient, FortiCloud, FortiCore, FortiMail, FortiSandbox, FortiADC, FortiAI, FortiAP, FortiAppEngine, FortiAppMonitor, FortiAuthenticator, FortiBalancer, FortiBIOS, FortiBridge, FortiCache, FortiCall, FortiCam, FortiCamera, FortiCarrier, FortiCASB, FortiCenter, FortiCentral, FortiConnect, FortiController, FortiConverter, FortiCWP, FortiDB, FortiDDoS, FortiDeceptor, FortiDirector, FortiDNS, FortiEDR, FortiExplorer, FortiExtender, FortiFirewall, FortiFone, FortiGSLB, FortiHypervisor, FortiInsight, FortiIsolator, FortiLocator, FortiLog, FortiMeter, FortiMoM, FortiMonitor, FortiNAC, FortiPartner, FortiPenTest, FortiPhish, FortiPortal, FortiPresence , FortiProtect, FortiProxy, FortiRecorder, FortiReporter, FortiSASE, FortiScan, FortiSDNConnector, FortiSIEM, FortiSDWAN, FortiSMS, FortiSOAR, FortiSwitch, FortiTester, FortiToken, FortiTrust, FortiVoice, FortiVoIP, FortiWAN, FortiWeb, FortiWiFi, FortiWLC, FortiWLCOS and FortiWLM.*

Outras marcas pertencem aos seus respetivos proprietários. A Fortinet não verificou independentemente declarações ou certificações aqui atribuídas a terceiros e a Fortinet não endossa independentemente tais declarações. Não obstante qualquer disposição em contrário aqui contida, nada aqui constitui uma garantia, contrato, especificação vinculativa ou outro compromisso vinculativo da Fortinet ou qualquer indicação de intenção relacionada com um compromisso vinculativo, e as informações de desempenho e outras especificações aqui contidas podem ser exclusivas para determinados ambientes. Este comunicado à imprensa pode conter declarações prospetivas que envolvam incertezas e suposições, tais como declarações relativas a divulgações de tecnologia, entre outras. Alterações de circunstâncias, atrasos na divulgação de produtos, ou outros riscos, tal como indicado nos nossos arquivos na Securities and Exchange Commission, localizada em www.sec.gov, podem fazer com que os resultados sejam materialmente diferentes dos expressos ou implícitos neste comunicado de imprensa. Se as incertezas se materializarem ou os pressupostos se revelarem incorretos, os resultados podem diferir materialmente daqueles expressos ou implícitos por tais declarações e pressupostos prospetivos. Todas as declarações que não sejam declarações de factos históricos são declarações que podem ser consideradas declarações relativas ao futuro. A Fortinet não assume qualquer obrigação de atualizar quaisquer declarações relativas ao futuro, e renuncia expressamente a qualquer obrigação de atualizar estas declarações relativas ao futuro.

**Para mais informação contacte:**

**Lift Consulting**

Erica Macieira | erica.macieira@lift.com.pt | 910549515

Inês Filipe | ines.filipe@lift.com.pt | 910 283 054