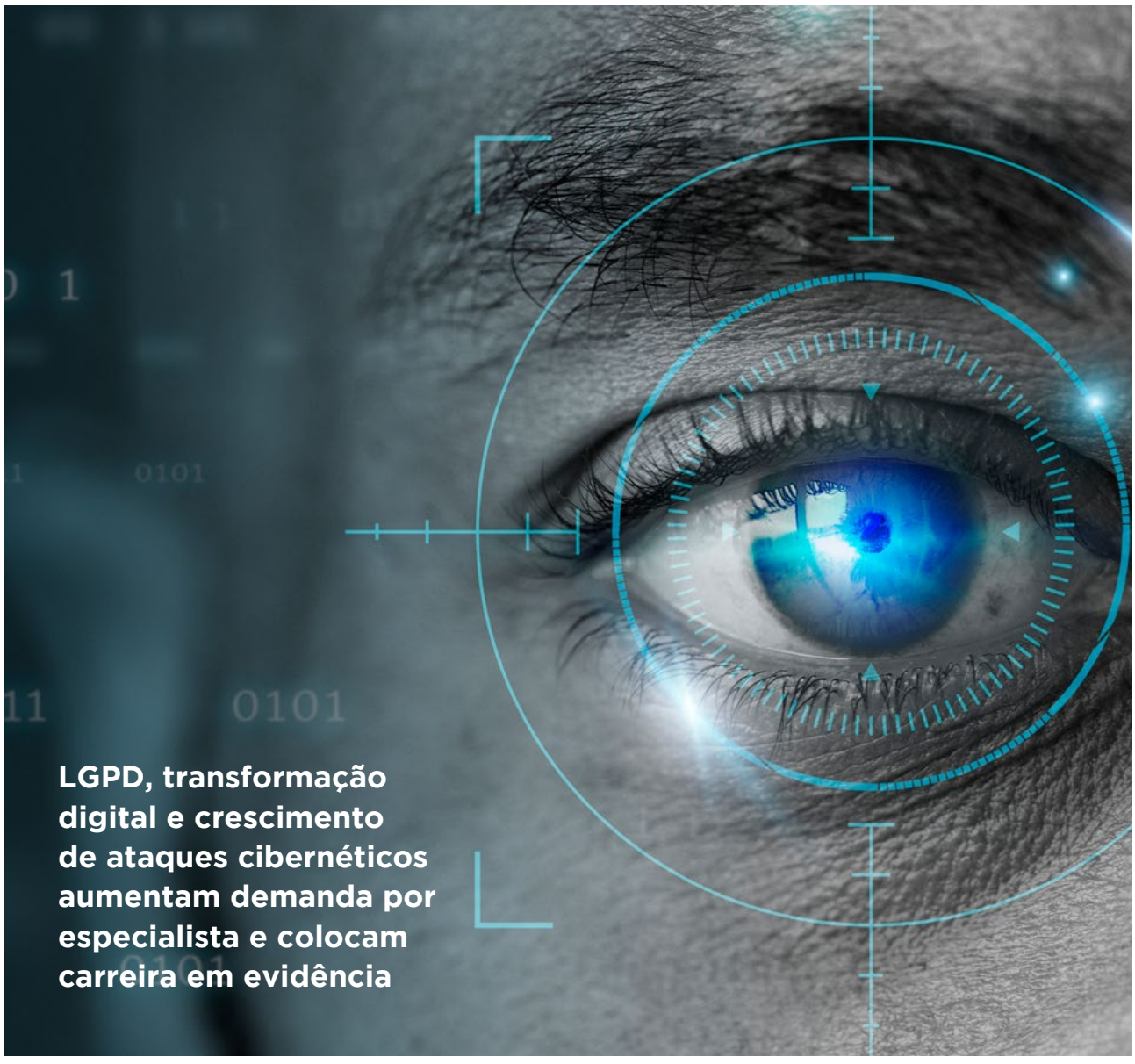
eu CAPACITO

E-BOOK GRATUITO

CIBERSEGURANÇA

De onde vem e para onde vão os profissionais de segurança da informação



De figura enigmática, vestindo uma toca na cabeça de frente ao computador em um ambiente escuro, ao especialista que se tornou indispensável para proteger as empresas diante do aumento de ataques de hackers, ransomware e vazamentos de dados. O profissional de cibersegurança é hoje uma das carreiras mais promissoras na área de tecnologia. De acordo com estimativas da Cybersecurity Ventura, empresa de pesquisas de cibereconomia, a área deve gerar 3,5 milhões de postos de trabalho globalmente até o fim de 2021.

No Brasil, além da aceleração da transformação digital das empresas, a aprovação da Lei Geral de Proteção de Dados (LGPD), em 2018, intensificou a demanda por esses especialistas. Outro fator também aponta para necessidade de profissionais: o País está na mira dos cibercriminosos, sendo o quinto no mundo que mais sofreu ataques de ransonware no primeiro trimestre de 2021, segundo a SonicWall.

Os profissionais de cibersegurança são responsáveis por planejar, gerenciar e implementar técnicas de defesa cibernética nas organizações dos mais diversos segmentos. Verdadeiros guardiões da informação, possuem alta capacidade analítica para identificar ameaças e vulnerabilidades nos sistemas e reagir prontamente com uma solução eficiente perante problemas complexos.

Para tanto, é imprescindível ter uma boa base técnica de proteção contra ataques e dominar a área de tecnologia de forma holística. Raciocínio lógico, habilidade com números e uma visão analítica aguçada também são cruciais. Vale lembrar que a área de segurança cibernética vem se tornando cada vez mais interdisciplinar, ao passo que trabalha diretamente para endereçar demandas das áreas de negócio, exigindo boas habilidades de gestão, planejamento e comunicação.

Os profissionais de cibersegurança, de modo geral, têm uma formação em Sistemas da Informação ou Ciências da Computação. São orientados para exatas – logística, estatística e a base técnica devem estar enraizadas. “São profissionais curiosos, que gostam de aprender, autodidatas, bons de lógica e, sobretudo, entendem de arquitetura de TI como um todo, bem como as aplicações se conversam e como se dão os fluxos de informação”, observa Raphael Carriço, gerente da divisão de Tecnologia da Michael Page.

Neste e-book, você conhecerá mais sobre essa profissão cada vez mais em alta, as habilidades necessárias para conquistar uma oportunidade em segurança digital ou até mesmo promover uma virada de carreira.

Capítulo 1
Histórico da profissão

Há cerca de 30 anos, se uma empresa possuía um antivírus e um firewall ela estava segura, já que as redes eram restritas aos escritórios e não se comunicavam com o mundo de fora. Nesse contexto, os profissionais de cibersegurança precisavam de alguma formação em Ciências da Computação ou Engenharia, com um misto de conhecimento de banco de dados, desenvolvimento e mainframe, para manter uma organização protegida.

“Antes não havia uma graduação específica, nem pós-graduação para quem queria trabalhar na área. Essas pessoas geralmente vinham de outras formações relacionadas à informática e engenharia. Elas estudavam as bases e aplicavam”, lembra Vinícius Vieira, coordenador acadêmico do curso de Defesa Cibernética da FIAP que atua há mais de 20 anos na área de cibersegurança.

Engenheiro civil de formação, Roberto Rebouças, gerente-executivo da Kaspersky no Brasil, enxergou no início de sua carreira uma oportunidade de utilizar seus conhecimentos analíticos para ingressar na área. “Naquela época os bancos contratavam engenheiros principalmente porque não existia uma formação de tecnólogos e foi onde comecei a trabalhar com plataformas, há 30 anos”. Foi, então, que migrou para o lado do fornecedor até ingressar na área de cibersegurança onde atua há 16 anos, compartilhou o líder de uma das maiores empresas de segurança digital do mundo.

Roberto Rebouças

O mercado de segurança no Brasil é relativamente novo, com pouco mais de 20 anos. Antigamente, bastava um profissional para dar conta de toda estratégia de segurança da informação de uma companhia. Hoje existem empresas com equipes de mais de cem pessoas somente de cyber, cada uma atuando em uma disciplina específica.

Carreiras em cibersegurança

Especialista em segurança: responsável pela segurança geral dos dados de uma empresa. Protege os sistemas contra vulnerabilidades e monitora as políticas de segurança.

Criptógrafo: lida com algoritmos e sistemas de segurança protegidos por criptografia. Gerencia códigos e realiza a proteção contra ataques cibernéticos.

Analista de segurança: implementa protocolos de segurança e conduz auditorias em toda a arquitetura de TI. Sua missão é identificar vulnerabilidades ou falhas na estrutura digital a fim de evitar invasões e perdas de dados.

“Pentester”: também conhecidos como hackers éticos, invadem sistemas computacionais a fim de testar a segurança. Esse trabalho é fundamental para indicar possíveis falhas e problemas aos negócios.

Arquiteto de segurança: são os oficiais de segurança de alto nível dos departamentos de TI. Planejam e projetam as estruturas de segurança com intuito de antecipar e mitigar atividades de hackers.

Especialista forense: são acionados após uma violação de segurança para analisar as evidências e identificar infratores. Possuem ampla visão de aspectos legais e dominam técnicas de investigação digital.

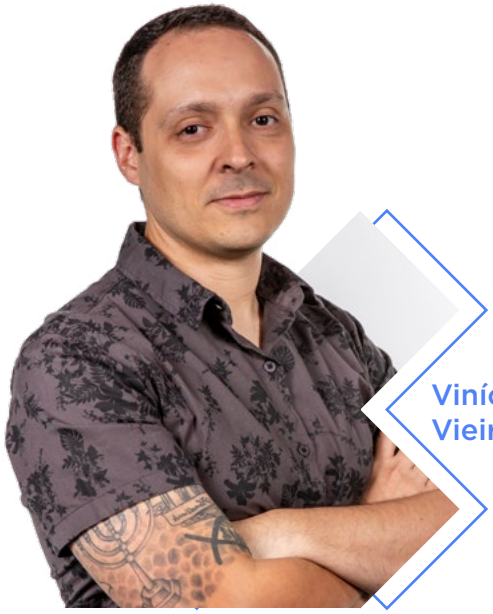
CISO (Chief Information Security Officer): o mais alto cargo em cibersegurança. É o executivo sênior responsável por estabelecer a visão, a estratégia e o programa de segurança digital da empresa para que todos os ativos sejam protegidos. Reporta diretamente para a presidência da empresa e trabalha em conjunto com os líderes de outras áreas.

Capítulo 2
Evolução da profissão

Com o avanço da internet e da transformação digital, os ambientes corporativos tornaram-se multiplataforma e interconectados com sistemas e softwares em nuvem, redes externas, dispositivos e IoT. Em contrapartida, ficou ainda mais complexo para os profissionais de segurança gerenciar e proteger toda essa infraestrutura e garantir a integridade das informações.

Os dados passaram a ser coletados e armazenados em sistemas locais e na nuvem em escala de petabytes, criando arsenais de informações (Big Data) sobre interações físicas e digitais relacionadas a clientes e a processos de gestão. Essas "minas de ouro" são alvos visados por cibercriminosos que desenvolvem técnicas sofisticadas de ataques para invadir sistemas, comprometer redes e roubar dados. Muitas vezes, esses dados são vendidos no mercado ilegal e até mesmo sequestrados com pedidos milionários de resgate.

Eis que chegamos a 2020: em meio a um cenário de pandemia e isolamento social, todas as empresas precisaram garantir que seus funcionários


Vinícius Vieira

trabalhassem de casa para manter as operações funcionando. “A Covid-19 colocou o profissional de cibersegurança em destaque porque toda a força de trabalho está online. A maturidade digital dos usuários não evolui no mesmo ritmo e muitos se tornaram vítimas de armadilhas de criminosos digitais, aumentando a superfície de ataque das empresas”, complementou Vinícius Vieira, da FIAP.

O resultado: um aumento de 330% no número de tentativas de ataques cibernéticos foi registrado no Brasil em 2020 pela Kaspersky. Não é à toa que a segurança digital tornou-se prioridade para mais de 80% das empresas, segundo o Barômetro da Segurança Digital 2021, realizado pelo Datafolha.

E para dar conta desta realidade complexa, a qualificação nas áreas de segurança, seja nos níveis mais juniores até o gerencial, passou a ser exigida pelas empresas. Por conseguinte, começaram a despontar cursos de graduação e pós-graduação de universidades e faculdades nos últimos anos, com foco em uma formação sólida e atualizada.

“A área de segurança é um macrotema, que envolve também disciplinas de área de tecnologia e gestão. Na graduação tecnóloga, no primeiro ano o aluno recebe toda a base teórica de segurança, aplicações, arquitetura, governança, enquanto o segundo ano é voltado para técnicas de segurança defensiva e ofensiva, análises de malwares e outras ameaças, bem como para as competências de inteligência artificial”, compartilha o coordenador acadêmico do curso de Defesa Cibernética da FIAP, que foi criado em 2018 e este ano conta com 257 alunos. “A demanda pelo curso tem aumentado assustadoramente”, completa.

Já o curso de pós-graduação em cibersegurança oferecido pela instituição na modalidade MBA, é cada vez mais buscado por profissionais de outras áreas além da tecnologia, principalmente do Direito – que procuram aliar os conhecimentos de especificidades da LGPD com uma formação específica em cyber para fazer uma virada de carreira.

A entrada de profissionais com diferentes formações nesta área também é observada por Alex Aguiar, sócio de cibersegurança da EY Brasil. “No passado, os profissionais de cibersegurança vinham das áreas de tecnologia e de controle e atualmente a disciplina atrai profissionais de diversas áreas. A transformação digital está levando as pessoas do jurídico e de negócios para a segurança a fim de trilhar uma carreira na área de privacidade”, pontua.

E para quem busca uma oportunidade, a recomendação é decidir desde o início se pretende atuar com foco mais técnico ou estratégico. “Naturalmente, o profissional de segurança digital tem um perfil curioso e criativo, e terá que buscar uma especialização, seja por meio cursos e certificações na área”.

Entre as principais certificações disponíveis, merece destaque a certificação básica da Security+ da CompTIA, compatível com os padrões ISO 17024 e aprovada pelo Departamento de Defesa dos EUA, que fornece uma visão geral para quem deseja consolidar uma carreira em segurança de TI.

As oportunidades são tanto para empresas tradicionais, quanto startups dos diversos setores da economia, com destaque para o setor financeiro, telecomunicações, indústria e saúde

Mulheres na cibersegurança

Assim como em toda área de tecnologia, as mulheres também são minoria nos postos de trabalho de segurança cibernética. Historicamente, elas não foram incentivadas a seguir áreas de exatas e, por questões culturais, o trabalho feminino sempre foi associado a habilidades como cuidado, criatividade e pessoas. Esses estereótipos estão sendo quebrados aos poucos, mas ainda há um longo caminho a ser percorrido, principalmente no que diz respeito à equidade de salários e na progressão de carreira até os cargos de liderança.

Conheça duas mulheres que enfrentaram o preconceito de uma área majoritariamente masculina e hoje ocupam cargos de liderança em empresas de cibersegurança.

Vanessa Pádua, diretora de cibersegurança da Microsoft para a América Latina e Caribe

Em 2009, Vanessa foi a primeira mulher na América Latina a obter a certificação Certified Information Systems Security Professional – CISSP, uma das mais importantes para a área. Ela também recorda que tanto na graduação em Sistemas da Informação, quanto no mestrado em Engenharia da Computação havia apenas outras duas mulheres em sua turma.

De estagiária em tecnologia na área de arquitetura de redes, logo passou a atuar no suporte e depois no pós-vendas, área em que também teve sua primeira experiência como líder, em uma consultoria de TI.

Hoje, além de liderar a divisão da segurança digital da gigante de tecnologia Microsoft no Brasil, ela busca inspirar outras a seguirem uma carreira em TI, uma vez que é líder de talentos do programa Women in Cybersecurity, organização que promove profissionais mulheres na área de cibersegurança.

“A área de segurança é para todos e todas. Não queremos ser a primeira, queremos ser muitas. Várias mulheres desejam ingressar em cibersegurança mas não sabem como chegar, por isso um dos pilares da ONG é a mentoria, em que mulheres mais experientes aconselham as mais jovens como trilhar um caminho de sucesso”, comenta.

Às mulheres que aspiram ingressar na área ou alcançar cargos de liderança, Vanessa recomenda buscar por esse apoio em diversos programas e organizações de incentivo às mulheres na tecnologia. “Precisamos de diversidade nos times, pois assim conseguimos enxergar melhor os problemas e endereçar as soluções.”

Daniela Costa, vice-presidente para a América Latina da Arcserve

Aos 19 anos, Daniela ainda cursava administração quando decidiu que queria trabalhar no mercado de tecnologia. Ingressou como estagiária de vendas da área de segurança da CA Technologies até chegar ao atual cargo de liderança ocupado na Arcserve, companhia especializada em proteção de dados.

Percorrer distintas funções ao longo de uma carreira de 23 anos, em posições que vão do marketing à distribuição, lhe trouxe uma bagagem ampla, que foi complementada com treinamentos em segurança. “Há muitas posições nesse mercado, especialmente em canais e revendas, em que você não precisa de uma formação em engenharia ou sistemas de informação, e sim de seguir um processo e fazer as perguntas certas”.

Assim, ela recomenda às outras mulheres que realizem cursos especializados, desenvolvam habilidades interpessoais e a capacidade de trabalho em equipe, sejam curiosas e, sobretudo que dominem o idioma inglês.

Hoje, Daniela é mãe de trigêmeos e ressalta que foi fundamental contar com o apoio de uma chefe mulher, que inclusive a promoveu durante a maternidade.

Capítulo 3
Toda empresa precisa de um guardião

Um déficit de aproximadamente 150 mil profissionais de Tecnologia da Informação, incluindo cibersegurança, é o tamanho do desafio enfrentado pelas empresas na hora de preencher suas vagas, estima o IDC. Somente em julho de 2021, mais de 180 vagas em cibersegurança foram abertas no LinkedIn, revela a empresa de recrutamento e seleção Michael Page, que possui uma parceria com a rede social profissional.

Raphael Carriço, gerente da divisão de Tecnologia da Michael Page, conta que há em média cerca de 30 vagas em segurança digital abertas no grupo, sendo que 40 contratações foram concluídas recentemente. Ele lista quatro fatores como impulsionadores desta demanda: home office e o trabalho híbrido impulsionados pela pandemia; a digitalização dos negócios; o aumento dos ataques cibernéticos; e a LGPD.

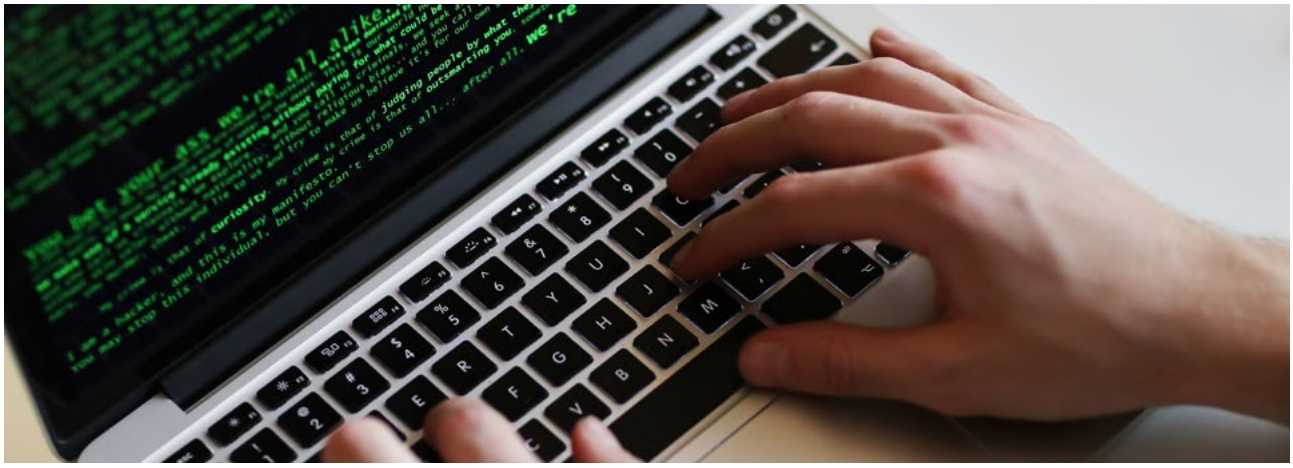
“Os salários estão inflacionados porque é difícil recrutar, sem contar que a alta remuneração é uma saída para reduzir o turnover e manter os profissionais engajados, visto que eles são extremamente disputados. No geral, a tecnologia é o mercado que mais cresce em termos de vagas”, analisa Carriço.

Cibersegurança: os três principais perfis profissionais

Corporativo: profissional que analisa as regras de segurança e atuam de forma consultiva, balizados por regras e normas, como LGPD, ISO 27001 e outras);

Técnico/forense: perfil mais técnico que administra o parque tecnológico para garantir um ambiente seguro). Concentra o maior volume de vagas;

Administrativo: voltado para análise de problemas e aplicações de medidas para garantir que a integridade dos sistemas por meio do gerenciamento de acessos e permissões.



Quanto às faixas salariais, as médias oferecidas pelas vagas para quais a Michael Page realiza o recrutamento são de: a partir de R$ 5 mil para o nível júnior; R$10 a R$20 mil para analistas; acima de R$ 20 mil para cargos gerenciais.

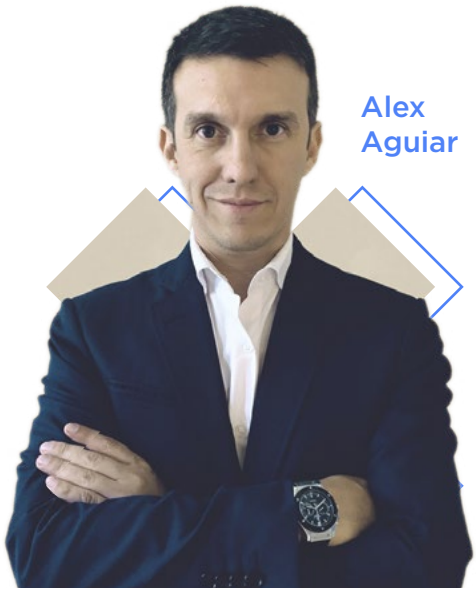
As oportunidades são tanto para empresas tradicionais, quanto startups dos diversos setores da economia, com destaque para o setor financeiro (que tornou-se ainda mais digital na pandemia e sofrerá uma verdadeira revolução com a virada para o open banking) telecomunicações, indústria e saúde. Este último, passou por um intenso processo de digitalização durante a pandemia e despontou como a área mais vulnerável a ataques cibernéticos no ano passado, seguido por educação, aponta Barômetro da Segurança Digital.

Capítulo 4
Para além do conhecimento técnico

À medida que a segurança ganha relevância nas organizações, o perfil do profissional deixa de ser puramente técnico e passa exigir soft skills (habilidades interpessoais), como capacidades de planejamento para priorizar os investimentos e otimizar gastos. “Sem contar que este profissional terá sempre que se manter atualizado, pois as ameaças avançam no mesmo ritmo das tecnologias”, afirma Alex Aguiar, da EY Brasil.

Roberto Rebouças, da Kaspersky no Brasil, compara a formação específica para área de segurança como a de um clínico geral. “O profissional deve ir além e investir em si mesmo para crescer, buscar especializações e tirar certificações”. Outro ponto fundamental é autoconfiança. “Não é uma área que você pode trabalhar se for uma pessoa indecisa. Muitas vezes, você toma atitude com pouca ou quase nenhuma de informação, pois é preciso agir rapidamente diante de um ataque cibernético”.

Para Carriço, o profissional que desenvolver as soft skills terá sucesso em qualquer projeto. “Cerca de 99,9% dos requisitos para as vagas estão relacionados a habilidades de comunicação com o time. Não adianta ser aquele funcionário que vai colocar o fone e ficar no computador, pois a TI atua cada vez mais de forma colaborativa com as áreas de negócio”.


Alex Aguiar

No fim do dia o propósito é o mesmo: a tecnologia pelo negócio. “Então é importante saber ouvir e fazer boas perguntas. O domínio do inglês também é mandatório, uma vez que as principais linguagens de programação e tecnologias são baseadas no idioma”, adiciona.

Para driblar a falta de mão de obra, as companhias têm optado por capacitar internamente. Na EY (antiga Ernst Young), por exemplo, cerca de 30 trainees realizam o programa de formação interna anualmente, no qual recebem certificações de seguran-

ça, passam por uma trilha de conhecimento e são orientados por especialistas em coaching de carreira.

“Há muita demanda no mercado de trabalho, mas as empresas hoje buscam não apenas alguém com conhecimento em segurança, mas sobre o setor em que elas atuam”, frisa Alex Aguiar, sócio de cibersegurança da EY Brasil. Dessa forma, o profissional será capaz de traduzir o risco da ameaça para o negócio e planejar os recursos necessários para definir controles e proteções internas.

Rebouças lembra que há 20 anos o responsável pela segurança era considerado a pessoa do “não”, que não permitia que os outros pares instalassem aplicações nos computadores para evitar riscos. “Hoje ele tem que ser a pessoa do ‘sim’, viabilizar a entrega de novos produtos e inovações que impulsionarão a competitividade”.

Não adianta ser aquele funcionário que vai colocar o fone e ficar no computador, pois a TI atua cada vez mais de forma colaborativa com as áreas de negócio” Raphael Carriço, da Michael Page.

Tanto que o profissional de cibersegurança passou a ocupar uma cadeira no C-level, participando das decisões estratégicas do negócio. Novamente, fica claro que a área de cibersegurança está cada vez mais atrelada ao negócio.

“Segurança por si só não se sustenta se você não entender do negócio da empresa”. Por isso, Rebouças acredita é importante enxergá-la a partir da análise do risco e definir o que viabilizar ou não – daí a importância das soft skills. Em uma analogia simples: não adianta colocar um carro na rua e adicionar o airbag ou para-choque somente depois de bater. O mesmo vale para um sistema de e-commerce, se uma empresa não quer sofrer um ataque de ransomware.

“O que a gente aprende fácil, a gente esquece fácil. Tem que quebrar pedra para que aquele conhecimento fique enraizado. Não basta ficar só no livro, é preciso pôr a mão na massa”, compartilha o gerente-executivo da Kaspersky. “Mesmo hoje eu ponho a mão na massa e posso até ganhar do meu engenheiro”, brinca.

Dicas valiosas para um caminho de sucesso em cibersegurança

1. **Busque mentorias com profissionais da área:** há diversas ONGs e projetos sociais que apoiam novos talentos na jornada de formação em cibersegurança, como a Women in Cybersecurity, na qual Vanessa Pádua, diretora de cibersegurança da Microsoft para a América Latina e Caribe, atua como líder.

2. **Domine as tendências atuais:** atualmente o profissional mais visado em segurança digital hoje é aquele que conhece de segurança de nuvem e governança de dados, áreas que vêm ganhando destaque frente à realidade do trabalho híbrido e às exigências da LGPD.

3. **Fique de olho nas próximas ondas:** em um contexto de rápida evolução da tecnologia, a executiva acredita que duas tendências emergirão nos próximos seis meses e influenciarão nas dinâmicas do profissional de cibersegurança: a ciência de dados e a computação quântica.

4. **Lembre-se das soft skills:** além do conhecimento técnico e do idioma inglês, comunicação, pensamento crítico, capacidade de planejamento e autoconfiança também são importantes para o profissional dessa área.

Sobre o Eu Capacito

O Eu Capacito é um projeto social que tem o objetivo de formar uma legião de profissionais para a economia digital. Apoiado por diversas empresas da iniciativa privada, a plataforma Eu Capacito promove a capacitação profissional gratuita, focadas em habilidades de tecnologia, seja do ponto de vista conceitual, técnico (desenvolvimento) ou ferramental (manuseio para áreas de negócio), além de conhecimento em outras áreas consideradas importantes para a vida corporativa ou empreendedorismo (soft skills). Criado pelo Movimento Brasil Digital, atualmente o projeto é liderado pelo Instituto IT Mídia, organização sem fins lucrativos dedicada a projetos educacionais de impacto na área de tecnologia da informação.

CONHEÇA O EU CAPACITO

Sigam nos, nas redes sociais

eu CAPACITO

Av. Engenheiro Luís Carlos Berrini, 105 - Cidade Monções, São Paulo - SP, 04571-010