

Em um mundo cada vez mais digitalizado, onde a informação se tornou um dos ativos mais valiosos, a segurança cibernética transcende a esfera tecnológica para se consolidar como um pilar fundamental da governança e da sobrevivência de qualquer organização. Esse foi o tema central do webinar "Horizontes da APEP", realizado em 26 de junho em parceria com o IPCOM, que reuniu especialistas de diversas áreas para desmistificar o conceito de segurança da informação e ressaltar sua importância vital para as Entidades Fechadas de Previdência Complementar (EFPCs).

Mediador do evento, **Herbert de Souza Andrade**, Presidente da APEP, abriu o debate destacando a crescente curiosidade e as muitas dúvidas – e mitos – que cercam a segurança da informação. “Não se trata apenas de senhas longas e firewalls, mas de governança, cultura, prevenção e responsabilidade institucional”, afirmou.

A Complexa teia de riscos globais e locais

Thiago Calçada, Diretor Executivo da área de Wealth da Mercer Brasil, trouxe um panorama impactante sobre os riscos globais, apresentando dados da pesquisa anual da Mercer, Marsh e Fórum Econômico Mundial. Ele enfatizou a "interconexão dos riscos", mostrando como ameaças aparentemente distintas, como desinformação e polarização social, podem estar ligadas a ataques cibernéticos. "Um dos principais riscos selecionados para 2025 é a desinformação ou falta de informação, ligada diretamente à tecnologia", ressaltou Thiago. Ele alertou que o Brasil é um alvo frequente de ciberataques, sendo o país na América Latina que mais sofre com softwares maliciosos.

Complementando a visão, **Francisco Fernandes**, Doutor em Controladoria e Contabilidade e sócio fundador da PFM, apresentou estudos sobre os riscos e controles no setor, revelando que, apesar de algumas melhorias, muitas EFPCs ainda exibem déficits significativos em controles básicos de segurança da informação. Francisco compartilhou exemplos de casos reais, como invasões a bancos de dados de EFPCs e patrocinadoras, que resultaram em roubo de informações sensíveis, vazamentos e até sequestro de dados com pedido de resgate. "A mecânica não escolhe você. Ela tenta com todos. Não pense que com você não vai acontecer", alertou, sublinhando que, em 2024, houve 921 trilhões de tentativas de atividades maliciosas na América Latina, um número assombroso que exige vigilância.

LGPD: A virada cultural na proteção de dados

O debate aprofundou-se na privacidade de dados com as contribuições de **Augusto Etchebehere Tavares de Tavares**, Gerente Executivo de Assuntos Legais e Regulatórios há 16 anos na Vivest, e **Marina dos Santos Vieira Fabro**, Sócia e Diretora Executiva da Data A e da MAPS+Data A. Augusto explicou que a Lei Geral de Proteção de Dados (LGPD) representou uma revolução cultural, forçando as empresas a tratarem dados pessoais com a seriedade que merecem. "A LGPD trouxe para o mundo do direito a proteção aos dados do indivíduo, da pessoa física", afirmou, detalhando princípios como finalidade, necessidade, segurança e transparência.

Augusto destacou a importância de distinguir entre controlador e operador de dados, um ponto crítico para as EFPCs que lidam com inúmeros prestadores de serviço. A negligência pode acarretar multas milionárias (até R\$ 50 milhões por infração), como ilustrado pelo caso do Facebook no Brasil. Marina ressaltou que a ANPD (Agência Nacional de Proteção de Dados) já tem regulamentação para reporte de incidentes, e a primeira sanção efetiva ocorreu em 2023. Ela também pontuou o risco de ter múltiplos sistemas fragmentados: "Muitos sistemas, cada um com seu banco de dados específico, ensejam riscos para a entidade, pois dificultam o rastreamento dos dados".

Ameaças comuns e a importância da conscientização humana

Os especialistas detalharam as ameaças mais comuns. Marina Fabro explicou que a segurança

cibernética se baseia em confidencialidade, integridade, disponibilidade e autenticidade. Ela diferenciou phishing ("ph", parece, mas não é) e whaling (ataques cibernéticos direcionados a altos executivos), e alertou para o crescimento do malvertising (publicidade maliciosa) e das vulnerabilidades em APIs (um quarto dos ataques em 2024 foram via APIs).

Evandro Luís de Oliveira, Diretor Executivo de Previdência e Investimentos da WTW Brasil, e **Ana Albuquerque**, especialista em riscos cibernéticos da WTW, reforçaram que o risco cibernético é um risco de negócio, não apenas de TI. Ana apresentou o fluxo de um ataque, desde o pré-ataque até o impacto financeiro, e destacou que, embora não se possa controlar quando um ataque ocorre, é possível controlar a resposta. A taxa de sucesso de 97% nos bloqueios de ataques em 2024 é positiva, mas a "severidade" dos 3% que passam é altíssima.

Relacionamento com fornecedores: uma responsabilidade compartilhada

A relação com fornecedores foi outro ponto crucial. Thiago Calçada enfatizou que a terceirização não transfere o risco, apenas o compartilha. "A responsabilidade não cai no CNPJ, cai no CPF do tomador de decisão", salientou. Ele destacou a necessidade de políticas bem estruturadas para seleção, contratação e monitoramento de fornecedores, além de auditorias e testes para garantir o cumprimento das cláusulas contratuais, especialmente com a solidariedade prevista na LGPD. Francisco Fernandes acrescentou que a contratação de provedores de TI de classe mundial pode melhorar o balanço de risco, mas exige due diligence e verificação periódica.

Boas práticas e o papel do seguro cibernético

O painel abordou práticas essenciais: autenticação multifator, cuidado com e-mails e dispositivos próprios, e a importância de não armazenar informações desnecessárias. Thiago Calçada reforçou a necessidade de treinamento contínuo e personalizado, utilizando ferramentas como "phishing do bem" para testar e educar os colaboradores.

Ana Albuquerque detalhou o funcionamento do seguro cibernético, apresentando-o como uma "estratégia operacional" para mitigar perdas financeiras. Ela explicou que o seguro cobre desde a resposta a incidentes (peritos forenses, negociação de extorsão) até a responsabilidade civil por vazamento de dados e perdas de receita por interrupção de negócios. Ela mostrou como avaliações de risco detalhadas (Assessment, Secure Scorecard, Cyber Quantifier) podem ajudar as empresas a entenderem sua exposição e até reduzir o custo do prêmio do seguro. "Não há risco zero", disse Ana, enfatizando que o objetivo é mitigar e diminuir ao máximo a probabilidade e o impacto.

Cultura de segurança e conscientização: o elo mais forte

O ponto culminante do webinar foi a unânime concordância sobre a primazia da cultura de segurança. Augusto Tavares defendeu que a alta liderança (Conselho Deliberativo, Diretoria Executiva) deve estar plenamente consciente de que segurança da informação não é um problema de TI, mas de negócio. A Vivest, por exemplo, mantém um Comitê de Segurança e Privacidade, treinamentos periódicos (incluindo testes de engenharia social) e comunicação constante. "A LGPD é um comportamento de todos os indivíduos", afirmou Augusto, ressaltando a necessidade de apoio ao empregado para esclarecer dúvidas e de um plano de ação para incidentes internos.

Evandro Oliveira exemplificou como a WTW desenvolveu sistemas para evitar o trânsito de dados sensíveis por planilhas e garantir que apenas informações necessárias sejam acessadas, minimizando a exposição. A conscientização se estende a todos, desde o mais alto escalão até o uso diário de ferramentas como o WhatsApp e a Inteligência Artificial.

Conclusão: um chamado à vigilância contínua

Ao final do evento, Herbert de Souza Andrade sintetizou a mensagem principal: "Segurança da informação não é só uma pauta técnica. É mais do que isso: é uma responsabilidade institucional." A jornada por dados protegidos, sistemas seguros e boas práticas é contínua e exige o

envolvimento de todos. O webinar deixou claro que, para navegar nos desafios do presente e do futuro, os fundos de pensão devem investir não apenas em tecnologia, mas sobretudo na construção de uma cultura sólida de segurança e conscientização, protegendo assim não só dados, mas as histórias, as pessoas e os propósitos que movem o setor.

Para rever os temas discutidos nesse webinar, [assista à gravação do evento aqui](#).

Fonte: [APEP](#), em 08.07.2025.