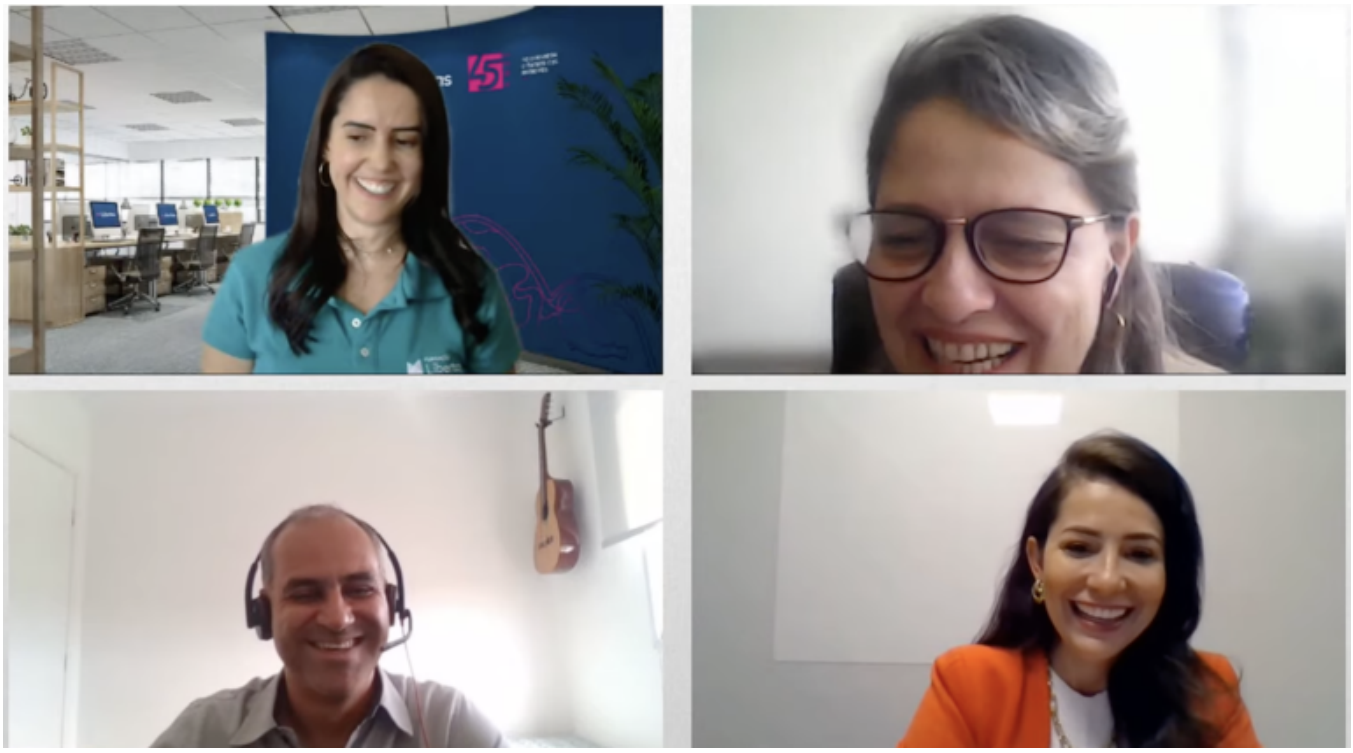
Rejane Rejo Tamoto



O conjunto de ações e técnicas para proteger de invasões e ataques virtuais as informações processadas, transportadas e armazenadas em equipamentos, sistemas e redes das EFPC é essencial para a mitigação de riscos e a continuidade dos negócios. A cibersegurança é uma responsabilidade que há muito deixou de ser apenas da área de Tecnologia da Informação – hoje deve ser compartilhada por todos os departamentos e níveis das entidades, do alto ao baixo escalão, já que o fator humano é o que faz a diferença no sucesso das medidas de proteção.

O tema foi abordado no webinar e lançamento do e-book “Cibersegurança: pontos de atenção e oportunidades de melhorias”, transmitido na tarde desta quinta-feira (16/02) no canal da Abrapp no Youtube. O evento foi organizado pela Comissão Técnica de Governança de Riscos da Regional Leste-Sudeste.

Na abertura do evento, o Diretor-Presidente da Abrapp, Jarbas Antonio de Biagi, lembrou que o segmento de Previdência Complementar Fechada é um sucesso em termos de proteção social e de pagamento de benefícios, mas que se perpetua por meio da confiança e segurança que os participantes e assistidos têm no trabalho das entidades. “Para responder a essa confiança, temos que cuidar da segurança desse contrato, principalmente do que é mais valioso para os participantes, que são os dados e informações. Eles são invioláveis e protegidos juridicamente”, afirmou.

Segundo o Diretor-Presidente, a pandemia trouxe a aceleração da transformação tecnológica e, com isso, a necessidade de adoção de instrumentos de segurança para a proteção contra a violação de dados. “As EFPC têm dados sensíveis e deve ser nossa preocupação instrumentalizar para que não sejam acessados sem autorização, e os sistemas de tecnologia não sejam violados. É um trabalho de melhoria contínua que a Abrapp faz, por meio da Comissão de Gestão de Governança e Riscos. Nesse ponto, sabemos que algumas entidades estão mais avançadas e outras se aperfeiçoando cada vez mais. Por isso, neste evento de lançamento do e-book compartilhamos o que temos de melhor para a preparação e aperfeiçoamento de todos. Os participantes se sentem seguros porque sabem que estamos envolvidos no processo de melhoria contínua”, pontuou Jarbas de Biagi.

Durante o evento, os especialistas que participaram da elaboração do e-book Juleika Cristina Ferreira de Carvalho (Coordenadora Suplente da CT Leste-Sudeste), Hubner Nazário Braga (membro da CT Leste-Sudeste) e Tatiane Baía Rodrigues (Gerente de TI da Fundação Libertas), apresentaram, de forma didática, os principais pontos de um trabalho que começou há dois anos.

O e-book teve foco em metodologias, em uma linguagem que possibilitasse a implementação pelas áreas técnicas das entidades. “Esse é um tema preponderante e que está na pauta estratégica. Frequentemente temos notícia de invasões e de sequestro de dados. Em entidades fechadas, esse tipo de situação pode trazer dor de cabeça não só pela possível ruptura de serviços prestados, mas também um prejuízo enorme aos participantes se ocorrer próximo ao dia de pagamento”, lembrou Adriana Carvalho**,** Secretaria-Executiva do Colégio de Coordenadores da Comissão de Governança e Riscos, que foi a moderadora do evento. Segundo ela, antes mesmo da Lei Geral de Proteção de Dados (LGPD), a Abrapp estava atenta ao tema.

O fator humano é crucial

A Coordenadora Suplente da Comissão Técnica de Governança de Riscos da Regional Leste-Sudeste, Juleika Cristina Ferreira de Carvalho (Aceprev), explicou como funciona o processo de governança de dados e de cibersegurança e que ambos estão ligados à privacidade de dados. Segundo ela, o ataque cibernético é uma prática utilizada por hackers para acessar de forma não autorizada redes, servidores, sistemas operacionais, softwares e redes com objetivos distintos, desde alterar, impedir, deletar ou sequestrar dados. Os ataques mais recorrentes são os phishings, links maliciosos, e o ransomware, um malware que captura dados, criptografa e gera uma indisponibilidade dos dados, comprometendo a adequação à LGPD.

“É um ataque que fere um dos pilares da segurança da informação, que é a disponibilidade, trazendo transtorno às entidades”, afirma. Os pilares da segurança da informação são a integridade, confidencialidade e disponibilidade. A indisponibilidade merece um comunicado à ANPD – Agência Nacional de Proteção de Dados”, explicou.

O foco em segurança e privacidade se tornou uma responsabilidade social e um diferencial competitivo, ao qual as entidades devem estar adaptadas para garantir sua continuidade no sistema. Para a especialista, as EFPC precisam começar por um diagnóstico do ambiente tecnológico, processo que precisa ser repetido e atualizado com frequência, dada a rapidez com que as mudanças acontecem. Também é necessário um alinhamento de expectativas em relação ao planejamento estratégico, com a racionalização dos serviços de tecnologia. “No e-book trazemos dois frameworks conceituados no mercado, ISO27701 e Cys Controls, com temas como documentação, controle de processos e política e diretrizes que serão estabelecidas no ambiente”, afirmou.

A Coordenadora Suplente da CT Regional Leste-Sudeste destacou que o ponto crucial para o sucesso de um projeto nessa área é o fator humano, ou seja, conscientização e treinamento da importância de seguir as diretrizes de cibersegurança, voltado a todos os colaboradores, de todos os níveis. “Todos têm de saber as regras do jogo e se engajar nas práticas. Por isso, é importante que saibam os canais de comunicação”. A documentação de processos e a proteção de dados pessoais, com adequação à LGPD, são etapas requeridas para criar um programa de governança de dados de forma assertiva.

Procedimentos, softwares e seguro ciber

O membro da CT Governança de Riscos Regional Leste-Sudeste, Hubner Nazário Braga (Previdência Usiminas) disse que a Resolução CGPC 13 prevê no artigo 18 que os sistemas de informações gerenciais devem ser confiáveis e abranger todas as atividades da entidade, com procedimentos de contingência, segregação de funções entre usuários e administradores em sistemas informatizados, de forma que garanta integridade e segurança dos dados armazenados. “É tema que as entidades trabalham cada vez mais em função da revolução digital, que traz a reflexão da importância do processo e aprendizado sobre a gestão de risco”, afirmou.

Um dos pontos relevantes no processo é a gestão de contas e usuários, para o qual é preciso manter a guarda fechada, com ferramentas e soluções para mitigar riscos, como softwares de proteção de perdas de transmissão de dados e de bloqueio de transmissão para fora das entidades.

Outro ponto é a gestão de redes, que deve estar incorporada ao planejamento estratégico, desde a alta administração. “Com o home office, temos que fazer mais campanhas de segurança da informação aos colaboradores, para mitigar o risco de aberturas de portas às redes e às informações da entidade. Hoje também há o seguro ciber, no qual conseguimos obter alguma garantia de impacto que possa ocorrer na entidade”, explica.

Hubner Braga lembrou que no Seminário de Dever Fiduciário sobre Ética, Governança e Sustentabilidade, realizado no ano passado, a segurança cibernética ocupou o quinto lugar no ranking de riscos aos quais o sistema de previdência complementar fechado está exposto. “Por isso a importância de mitigar o risco com ações preventivas do que reparar os danos. É o melhor caminho para o tratamento da segurança da informação”, completou.

Desafios e mitos da cibersegurança

A Gerente de TI da Fundação Libertas, Tatiane Baía Rodrigues, apresentou os desafios, mitos e verdades sobre cibersegurança. Ela contou que a entidade sofreu um ataque de ransomware, que tornou os dados indisponíveis por dois dias. Ao todo, para se restabelecer do incidente, a Libertas levou 40 dias, em um episódio que trouxe muitos aprendizados.

Entre os desafios para que as entidades fortaleçam a cibersegurança, Tatiane Baía Rodrigues citou a complexidade, já que é preciso considerar todos os possíveis modelos de ataque virtual, os diferentes atacantes, objetivos e estratégias, bem como cenários. Outro ponto é a diversificação das formas de ataque, já que os hackers adotam estratégias criativas, profissionais, constantes e com potencial lesivo devastador. “O processo de transformação digital aumentou as complexidades do problema, já que convivemos com inteligência artificial, nuvem, computing IoT”, disse.

Outros desafios para a cibesegurança que ela observou são a baixa atratividade em termos de usabilidade, pois o processo exige verificação em vários níveis; o custo recorrente de manter sistemas e controles e, por fim, a baixa cultura organizacional em torno do tema. “Essa não é responsabilidade de uma área específica, mas de todos. A importância da prevenção é percebida, infelizmente, após ataques”, pontuou.

A gerente de TI da Libertas disse que o tema também é cercado de muitos mitos. Além da ideia de que a área de TI é a única responsável pela cibersegurança, há também a percepção de que apenas antivírus e sistemas são capazes de conter os ataques. “São mitos, já que o sucesso da segurança dependerá da cultura organizacional, do engajamento de conselheiros, diretores e todos os colaboradores. O grande ponto são as pessoas”.

Outro equívoco comum é colocar a responsabilidade da cibersegurança no compliance, com a ideia de que políticas e processos operacionais são suficientes. “É necessário também investimento em tecnologia, processos e treinamento de pessoal”. O quarto mito que a especialista citou foi de que as ameaças sempre vêm de fora, o que cai por terra quando na verdade também há a ameaça interna, ou seja, de quem acessa a plataforma privada. “O último ponto é que não é possível terceirizar totalmente a segurança cibernética. Pode ser um passo, mas não é tudo. Sempre será necessária a criação de cultura e conscientização de colaboradores”, conclui.

O e-book está disponível na biblioteca da Abrapp. Clique aqui **e garanta o seu exemplar.**

Fonte: Abrapp em Foco, em 17.02.2023.