Uma EFPC pode ter uma carteira de investimentos bem estruturada e, ainda assim, enfrentar dificuldades para pagar benefícios, acessar cadastros ou atender participantes. Basta que um sistema essencial fique indisponível, que informações sejam alteradas ou que um fornecedor interrompa seus serviços.

Essas situações podem decorrer de falhas internas, problemas técnicos ou eventos externos. Entre suas possíveis causas estão os ataques cibernéticos, que a inteligência artificial vem tornando mais rápidos e mais fáceis de executar. Diante disso, a proteção da EFPC não depende só da tecnologia. Passa também por decisões tomadas antes de um incidente ("evento"), por conhecer bem os prestadores de serviços essenciais dos quais ela depende e por saber como arcaria com os custos de uma eventual interrupção dos serviços.

A digitalização trouxe conveniência e agilidade. Consultar saldos, atualizar informações, requerer benefícios e encaminhar solicitações pela internet passou a integrar a experiência dos participantes, mas essas facilidades também ampliaram as conexões entre pessoas, sistemas e prestadores de serviços, e cada conexão exige cuidados com acesso, integridade dos dados e continuidade das atividades operacionais.

Com a inteligência artificial, esse ambiente muda de novo, e a mudança merece atenção mesmo nas EFPC que ainda não usam a tecnologia, porque quem ataca pode usá-la. As fraudes ajudam a perceber como esse risco chega à rotina da EFPC. Vozes e imagens produzidas artificialmente, combinadas com mensagens convincentes e informações sobre pessoas, podem dar aparência de legitimidade a uma solicitação falsa, feita em nome de um participante, de um dirigente ou de um fornecedor. Um pedido de alteração de dados bancários ou uma orientação de pagamento fora da rotina, por exemplo, exige verificação por outro meio de contato já conhecido pela EFPC, para confirmar se a solicitação partiu mesmo de quem diz tê-la feito. Reconhecer a voz ou o jeito de escrever de alguém já não oferece a mesma segurança de antes.

Em junho de 2026, o Fundo Monetário Internacional (FMI) publicou o estudo Artificial Intelligence and Cybersecurity in the Financial Sector, que analisa como a inteligência artificial está transformando os riscos cibernéticos no sistema financeiro. O estudo trata do setor como um todo, mas ajuda a entender a situação das EFPC, que dependem do mesmo prestador de serviços.

Segundo os autores, a inteligência artificial reduz o tempo necessário para executar ataques, facilita a superação de barreiras de proteção e permite que etapas de um ataque sejam realizadas com menor intervenção humana. Um levantamento da empresa de segurança CrowdStrike, citado no estudo, dá a medida dessa aceleração: o tempo que um invasor leva para avançar do primeiro equipamento invadido para outras partes da rede caiu, em média, para 29 minutos, 65% menos que no ano anterior.

Ataques mais rápidos exigem decisões preparadas. Quem deve ser avisado quando houver suspeita de um problema? Quem decide se um serviço precisa ser interrompido para evitar danos maiores? Como manter os pagamentos dos benefícios e o atendimento aos participantes enquanto a situação é resolvida? Se essas respostas só começarem a ser discutidas durante o incidente, a demora pode agravar suas consequências. Definir responsabilidades e combinar como agir faz parte da preparação da EFPC.

Essa preparação também precisa alcançar os prestadores de serviços, porque a exposição da EFPC não se limita ao seu ambiente interno. O estudo do FMI destaca o risco de concentração em terceiros, e ele também existe entre as EFPC: quando várias EFPC dependem do mesmo prestador para atividades essenciais, um problema nesse fornecedor pode comprometer muitas delas ao mesmo tempo. Mesmo com um bom prestador de serviços, a questão é saber o que aconteceria se ele ficasse indisponível e quanto tempo levaria para substituí-lo.

Há também dependências que não aparecem diretamente na relação com o fornecedor contratado. Duas empresas que oferecem sistemas para EFPC, por exemplo, podem utilizar a mesma plataforma de nuvem. Um evento inesperado (“incidente”) nessa plataforma pode afetar os dois fornecedores e, por consequência, as EFPC atendidas por eles. Contratar empresas diferentes, portanto, não elimina necessariamente a exposição a uma mesma origem de falha. E, se essa tecnologia compartilhada tiver uma vulnerabilidade, a inteligência artificial pode facilitar sua descoberta e acelerar ataques contra vários de seus usuários. Para a continuidade dos serviços, isso significa saber se o prestador de serviços conseguirá restabelecer o atendimento no prazo acordado quando muitos clientes precisarem dele ao mesmo tempo, e como serão mantidas as atividades essenciais durante essa espera.

Parte da resposta está nas cópias de segurança (“backup”), mas só tê-las não basta. Elas precisam estar protegidas e guardadas separadamente dos sistemas principais, para que um ataque a esses sistemas não alcance também as cópias, e sua recuperação deve ser testada. O tempo necessário para recuperar as informações precisa ser compatível com as atividades que dependem delas, como o pagamento de benefícios. Esses cuidados fazem parte dos controles internos da EFPC e precisam ter responsáveis definidos e acompanhamento periódico.

Controles internos diante dos novos riscos

A preocupação com controles internos nas EFPC antecede o debate atual sobre inteligência artificial. A Resolução CGPC nº 13/2004, estabeleceu princípios de governança, gestão e controles internos compatíveis com o porte, a complexidade e os riscos dos planos de benefícios sob gestão das EFPC. Entre outros pontos, a norma exige sistemas de informação confiáveis e prevê procedimentos de contingência e a segregação de funções entre usuários e administradores dos sistemas. Esses princípios valem para o cenário atual, e a própria Previc incluiu a segurança cibernética entre os temas de supervisão do seu Programa Anual de Fiscalização – FAF para 2026.

A proteção de dados acrescentou outras responsabilidades. A Lei Geral de Proteção de Dados Pessoais (LGPD) e o Regulamento de Comunicação de Incidente de Segurança, aprovado pela Resolução CD/ANPD nº 15/2024, exigem que a entidade avalie se um incidente pode causar risco ou dano relevante aos titulares dos dados. Quando for o caso, a comunicação à Autoridade Nacional de Proteção de Dados (ANPD) e aos titulares deve ser feita em até três dias úteis a partir do momento em que a entidade souber que dados pessoais foram atingidos, e todos os incidentes, mesmo os que não precisam ser comunicados, devem ser registrados. É pouco tempo para quem ainda está tentando entender o que aconteceu. Por isso, o plano de resposta precisa prever essas obrigações e seus prazos, com participação das áreas técnica, jurídica e de proteção de dados.

Mesmo com esses cuidados, permanece a possibilidade de interrupção dos serviços, exposição de informações e despesas inesperadas. Uma dificuldade no pagamento de benefícios ou um vazamento de dados pode exigir apoio especializado, recuperação de sistemas, orientação jurídica e comunicação com os participantes. Essas necessidades podem surgir ao mesmo tempo, quando a equipe já está dedicada a entender o ocorrido e a restabelecer as atividades. Além da capacidade de resposta, é preciso considerar como a EFPC suportaria os custos envolvidos.

O seguro cyber na gestão de riscos

É nesse contexto que o seguro de riscos cibernéticos, conhecido no mercado como seguro cyber, entra na gestão de riscos. Os controles internos reduzem a chance e o tamanho de um incidente, mas não o eliminam. O seguro atua sobre o risco que permanece: transfere para a seguradora parte das consequências financeiras e, conforme o produto, dá à EFPC acesso a profissionais especializados em resposta a incidentes. Para EFPC com equipes enxutas, que dificilmente manteriam essa estrutura por conta própria, esse apoio pode impactar tanto quanto a indenização. Sem seguro, a própria EFPC pode ter de arcar com as despesas de um incidente, com recursos que, em última instância, vêm dos participantes e patrocinadores.

Conforme os termos e condições de cada apólice, o seguro pode cobrir despesas como a

investigação técnica do incidente, a recuperação de dados e sistemas, a assessoria jurídica, as despesas de comunicação aos participantes, patrocinadores e à ANPD e o gerenciamento da crise de imagem, além da responsabilidade da EFPC por danos causados a terceiros, entre eles os próprios participantes e assistidos que tenham seus dados expostos. Alguns produtos incluem ainda os prejuízos decorrentes da paralisação dos sistemas e as situações de extorsão, como os ataques que bloqueiam os dados e exigem pagamento para liberá-los.

Por isso, apólices com limites semelhantes podem oferecer proteções e coberturas bem diferentes, e o preço ("prêmio") diz pouco sobre essa diferença. Alguns termos ajudam a fazer a comparação. O limite máximo de garantia é o teto da apólice; cada cobertura tem seu próprio limite máximo de indenização ("LMI"), e algumas trazem sublimites, valores menores reservados a um tipo específico de despesa. A franquia e a participação obrigatória do segurado ("POS") definem a parte do prejuízo que fica por conta da EFPC: a franquia costuma ser um valor fixo, e a POS, um percentual da perda. As exclusões indicam o que a apólice não cobre.

As coberturas de responsabilidade costumam ser contratadas à base de reclamações, o chamado claims made. Nesse formato, a apólice responde por reclamações apresentadas durante a vigência, ou nos prazos adicionais previstos no contrato, desde que os fatos tenham ocorrido entre a data de retroatividade e o fim da vigência. Também importam o prazo para avisar a seguradora sobre um incidente e, nas coberturas de paralisação, o período de espera, isto é, quanto tempo os sistemas precisam ficar fora do ar até que as perdas passem a ser indenizáveis. O próprio processo de contratação ajuda nessa análise, porque o questionário da seguradora sobre os controles da EFPC acaba funcionando como um diagnóstico da sua segurança.

Vale conferir também como a apólice trata os incidentes ocorridos em prestadores de serviços. A cobertura para esses casos depende das condições contratadas, e o seguro do próprio prestador não assegura proteção integral à EFPC. O mesmo cuidado se aplica à patrocinadora: sua apólice não necessariamente contempla a EFPC, e é preciso verificar quais organizações e riscos estão abrangidos pelo contrato.

O patrimônio administrado oferece contexto, mas não basta para dimensionar a proteção. A quantidade e a natureza das informações mantidas, a dependência de serviços externos e o impacto de uma interrupção ajudam a avaliar os recursos que poderiam ser necessários.

Também é importante saber, antes de qualquer problema, como o seguro será acionado: quem deve ser contatado, quais despesas dependem de autorização da seguradora e quais serviços de apoio estão disponíveis.

A confiança dos participantes e assistidos é construída ao longo de muitos anos. Por trás dos cadastros, dos saldos e dos pagamentos estão pessoas que contam com a EFPC para realizar seus sonhos e manter sua segurança financeira. Para os dirigentes e conselheiros, avaliar o seguro cyber faz parte da mesma diligência com que se avaliam os demais riscos da entidade. A inteligência artificial vem acelerando os ataques, mas boa parte da resposta continua nas mãos da própria EFPC, em decisões tomadas com antecedência. Prudência, tempestividade, diligência e proteção financeira caminham juntas para que a EFPC continue atendendo quem depende dela.

Danilo Moura é Sócio da Consepro

Fonte: Abrapp em Foco, em 11.11.2026.