

Instrumento de maturidade em segurança da informação em EFPC: desenvolvimento, avaliação exploratória e proposta de uso em supervisão baseada em risco

Leonardo Fiúza da Silva

Especialização em Privacidade e Segurança da Informação - Universidade de Brasília (UnB)

Orientador: Rafael Rabelo Nunes

rafaelrabelo@unb.br

Resumo. As Entidades Fechadas de Previdência Complementar (EFPC) dependem de dados, sistemas e serviços digitais cuja proteção exige governança, gestão de riscos e capacidade de resposta cibernética. O estudo desenvolveu um instrumento de maturidade em segurança da informação para esse contexto, examinou exploratoriamente sua estrutura interna e consistência e propôs diretrizes para uso futuro em supervisão baseada em risco. Realizou-se survey anônimo com profissionais do setor; dos 274 registros recebidos, 231 compuseram a amostra válida. Os 33 itens psicométricos foram examinados por estatística descritiva, consistência interna, correlações e análise fatorial exploratória (AFE). Os resultados sugeriram dois fatores correlacionados, associados à capacidade institucional de gestão e à cultura e ao comportamento seguro, coexistindo com uma forte dimensão geral. A consistência interna foi satisfatória na maioria dos domínios, embora o comportamento seguro requeira cautela e aperfeiçoamento. As associações previstas entre cultura, gestão de riscos, comportamento seguro e maturidade percebida apresentaram direção positiva. Os achados fornecem evidência exploratória sobre o funcionamento do instrumento, mas não permitem classificar EFPC, estimar criticidade institucional ou validar o uso supervisório proposto.

Palavras-chave: supervisão baseada em risco; previdência complementar fechada; maturidade em segurança da informação; cultura de segurança.

Abstract. Closed pension funds (EFPC) depend on data, systems, and digital services whose protection requires governance, risk management, and cyber incident response capabilities. This study developed an information security maturity instrument for this context, exploratorily examined its internal structure and consistency, and proposed guidelines for its future use in risk-based supervision. An anonymous survey was conducted with professionals in the sector; of the 274 records received, 231 formed the valid sample. The 33 psychometric items were examined using descriptive statistics, internal consistency estimates, correlations, and exploratory factor analysis (EFA). The results suggested two correlated factors, associated with institutional management capacity and with security culture and behavior, coexisting with a strong general dimension. Internal consistency was satisfactory for most domains, although the secure behavior domain requires caution and further refinement. The expected associations among culture, risk management, secure behavior, and perceived maturity were positive. The findings provide exploratory evidence on the functioning of the instrument but do not allow EFPC classification, estimation of institutional criticality, or validation of the proposed supervisory use.

Keywords: risk-based supervision; closed pension funds; information-security maturity; security culture.

1 INTRODUÇÃO

As Entidades Fechadas de Previdência Complementar (EFPC) administram planos previdenciários apoiados por dados, sistemas e serviços digitais. Na data de referência adotada pelo estudo, o universo institucional reunia 264 EFPC ativas, o que delimita o contexto regulado em que o instrumento foi concebido (Brasil, 2026b).

A dimensão socioeconômica reforça a relevância do segmento: ao final de 2025, o regime alcançava 8.684.418 pessoas vinculadas e administrava ativo total de R\$ 1,408 trilhão (Brasil, 2026d). Para dimensionar essa magnitude, esse estoque correspondia, em termos de valor, a aproximadamente 11,1% do Produto Interno Bruto brasileiro de 2025, de R\$ 12,7 trilhões (IBGE, 2026).

A supervisão desse segmento compete à Superintendência Nacional de Previdência Complementar (Previc), autarquia de natureza especial criada pela Lei nº 12.154, de 23 de dezembro de 2009, com atribuições de fiscalização e supervisão das EFPC e de suas atividades e operações (Brasil, 2009). Nesse contexto, riscos capazes de comprometer a continuidade operacional, a proteção das informações ou os interesses de participantes e assistidos também se inserem no ambiente de atenção do supervisor.

A relevância da segurança da informação decorre da combinação entre dados pessoais, ativos e dependência tecnológica. No setor de previdência privada, a International Organisation of Pension Supervisors (IOPS) identifica ameaças como phishing, malware, ransomware e engenharia social e aponta que ataques bem-sucedidos podem provocar perda de dados ou ativos, interrupção de serviços, descumprimento de deveres fiduciários, litígios e danos reputacionais (IOPS, 2021).

No Brasil, essa exposição não é apenas hipotética. Em 2020, a BB Previdência comunicou acesso não autorizado a uma transação em área restrita de seu portal, com possível acesso indevido a informações de 106 participantes. Segundo a entidade, não foram identificadas fraude ou movimentação que provocassem prejuízo às reservas previdenciárias (BB Previdência, 2020). O episódio não permite inferir a frequência de incidentes no segmento, mas evidencia que riscos relacionados à segurança da informação podem materializar-se também no ambiente das EFPC.

As entidades diferem em porte, complexidade, exposição tecnológica e capacidade de resposta. A supervisão baseada em risco procura ajustar a intensidade da atuação à materialidade e ao impacto potencial, evitando a distribuição uniforme do esforço fiscalizatório e direcionando maior atenção às situações de maior relevância (IOPS, 2023).

Essa perspectiva é particularmente pertinente à segurança da informação, pois entidades com características institucionais distintas podem apresentar diferentes combinações de dependência tecnológica, exposição e capacidade de gestão.

A segurança cibernética também passou a integrar explicitamente a agenda supervisória do segmento no Brasil. Para 2026, a Previc incluiu o tema entre os objetos de sua supervisão temática, evidenciando sua incorporação ao conjunto de riscos considerados na atuação supervisora (Brasil, 2026c).

Modelos de maturidade podem contribuir para esse contexto ao sintetizar o grau de institucionalização de práticas de segurança e permitir a identificação de aspectos que demandam maior atenção. Sua utilidade, entretanto, depende de adaptação ao ambiente estudado e de avaliação empírica do instrumento, evitando que pontuações sejam interpretadas como certificação ou evidência automática de conformidade (Brezavšek; Baggia, 2025).

Fatores humanos também influenciam segurança e conformidade. Cultura, percepção de ameaça, clareza de responsabilidades, engajamento e comportamento cotidiano podem favorecer ou limitar a efetividade das práticas institucionais, razão pela qual a análise da segurança não deve restringir-se à existência formal de políticas e controles (Delso-Vicente *et al.*, 2025).

A lacuna investigada situa-se na integração dessas vertentes para o contexto das EFPC brasileiras. O problema de pesquisa foi: como desenvolver um instrumento de maturidade em segurança da informação aplicável às EFPC e estruturar, a partir de seus escores, uma proposta de utilização futura em supervisão baseada em risco? Foram examinadas quatro hipóteses associativas: H1, cultura e engajamento em segurança associam-se positivamente à maturidade em gestão de riscos de segurança da informação; H2, essa maturidade associa-se positivamente ao comportamento seguro declarado; H3, cultura e engajamento em segurança associam-se positivamente ao comportamento seguro declarado; e H4, maturidade percebida associa-se positivamente aos demais domínios do instrumento e ao indicador composto de gestão de riscos. O objetivo geral foi desenvolver o instrumento, examinar exploratoriamente sua estrutura interna e consistência e propor diretrizes para utilização supervisória futura

Os objetivos específicos foram estruturar os domínios e itens, descrever os escores, examinar consistência interna e estrutura fatorial, testar as associações formuladas e delinear diretrizes para futura combinação dos escores com indicadores independentes de criticidade. O desenho não pretende validar uma regra de fiscalização, mas produzir evidência inicial

sobre o instrumento que poderia anteceder-lá. Os Apêndices A a E reúnem a rastreabilidade da construção do instrumento, o tratamento da base, resultados analíticos detalhados, o detalhamento da proposta de uso supervisorio e o instrumento aplicado.

A contribuição pretendida é, portanto, distinta da validação de um modelo fiscalizatório. O estudo produz resultados empíricos iniciais sobre um instrumento destinado a mensurar percepções relacionadas à maturidade em segurança da informação e, em camada aplicada separada, discute como esses escores poderiam futuramente ser combinados com informações institucionais independentes. Essa distinção preserva a utilidade prática da proposta sem atribuir aos dados coletados capacidade de classificar EFPC ou determinar respostas supervisoras.

2 REFERENCIAL TEÓRICO

2.1 Governança, gestão de riscos e maturidade

A ISO/IEC 27001:2022 trata a segurança da informação como sistema de gestão, integrando responsabilidades, avaliação de riscos, controles e melhoria contínua (ISO, 2022).

O Cybersecurity Framework (CSF) 2.0, do National Institute of Standards and Technology (NIST), reforça essa integração ao incluir a função *Govern* e relacionar decisões de segurança ao contexto, às responsabilidades e à supervisão organizacional (NIST, 2024).

A gestão de riscos também pressupõe identificação de ativos, ameaças, vulnerabilidades e impactos, seguida de tratamento, comunicação e revisão. Em ambientes terceirizados, o processo deve alcançar contratos, dependências tecnológicas, continuidade e responsabilidades compartilhadas, evitando que a gestão se restrinja à área de tecnologia (ISO, 2018).

Maturidade, nesse contexto, representa o grau de institucionalização das práticas. Revisões recentes mostram diversidade de modelos e alertam que pontuações só são úteis quando contextualizadas, examinadas empiricamente e vinculadas a decisões concretas (Brezavšček; Baggia, 2025).

O instrumento deste estudo utiliza os escores como síntese das práticas percebidas pelos respondentes, e não como certificação de conformidade. Esses escores não correspondem aos Tiers de Implementação do NIST CSF 2.0 e não permitem enquadrar uma EFPC como *Partial*, *Risk Informed*, *Repeatable* ou *Adaptive*. Também não substituem auditorias, avaliações de controles ou exames documentais; seus resultados devem ser

interpretados como sinais exploratórios a serem contextualizados com outras evidências (NIST, 2024).

Para a administração pública federal, o Programa de Privacidade e Segurança da Informação (PPSI) 2.0 constitui referência comparativa de governança, privacidade e segurança, sem ser tratado neste estudo como obrigação diretamente aplicável às EFPC (Brasil, 2026a).

2.2 Supervisão baseada em risco e proporcionalidade

A supervisão baseada em risco prioriza entidades, temas e ações conforme probabilidade, impacto, qualidade dos controles e capacidade de resposta. No setor previdenciário, a abordagem favorece atuação prospectiva e proporcional, mantendo requisitos mínimos comuns (IOPS, 2023).

No risco cibernético, a supervisão deve considerar governança, terceiros, incidentes, continuidade e evidências de efetividade, e não apenas a existência documental de controles (IOPS, 2021).

Proporcionalidade não significa flexibilizar indiscriminadamente controles essenciais. Mesmo entidades de menor porte podem apresentar exposição relevante em razão de volume e sensibilidade de dados, dependência de fornecedores, serviços digitais críticos ou histórico de incidentes; esses elementos devem influenciar a prioridade supervisória sem eliminar requisitos mínimos (IOPS, 2021).

A Previc segmenta as EFPC por porte e complexidade para fins de supervisão, fiscalização e proporcionalidade normativa. Para 2026, o enquadramento S1 a S4 foi atualizado pela Portaria PREVIC nº 539/2025 (Brasil, 2025).

2.3 Cultura de segurança e comportamento seguro

Políticas e ferramentas não asseguram, isoladamente, conformidade. Comportamentos seguros são influenciados por percepção de ameaça, eficácia das respostas, sanções e normas sociais (Herath; Rao, 2009).

A cultura de segurança conecta expectativas institucionais às práticas cotidianas. Liderança, comunicação, treinamento e clareza de responsabilidades influenciam o cumprimento de políticas, o relato de incidentes e a resistência a atalhos operacionais (Uchendu *et al.*, 2021).

Essa perspectiva explica por que avaliações exclusivamente documentais podem superestimar ambientes nos quais políticas existem formalmente, mas não foram incorporadas às rotinas. O inverso também é possível: comportamentos individuais favoráveis podem coexistir com fragilidades de governança, recursos ou processos, reforçando a necessidade de examinar conjuntamente dimensões institucionais e humanas (Uchendu *et al.*, 2021).

2.4 Trabalhos relacionados e lacuna de pesquisa

Foi realizada revisão narrativa orientada ao problema de pesquisa, sem pretensão de exaustividade. Os trabalhos examinados foram organizados segundo três vertentes diretamente relacionadas ao estudo: supervisão previdenciária baseada em risco, maturidade em segurança da informação e fatores humanos associados à segurança. O Quadro 1 reúne as fontes que mais diretamente sustentam essa articulação.

Quadro 1. Síntese das principais fontes relacionadas

Fonte	Foco	Contribuição	Limite
IOPS (2023)	Supervisão baseada em risco	Prioridade e resposta proporcional	Não define instrumento de maturidade em segurança da informação para EFPC
Brezavšček e Baggia (2025)	Maturidade em segurança	Contextualização e avaliação empírica	Não trata supervisão previdenciária
Delso-Vicente <i>et al.</i> (2025)	Fatores humanos	Base para cultura e comportamento	Não integra criticidade supervisória
Ferreira <i>et al.</i> (2025)	Controles cibernéticos no setor financeiro	Base setorial complementar	Não desenvolve escala para EFPC

Fonte: elaboração própria a partir das fontes listadas.

Na vertente supervisória, o IOPS (2023) fornece a lógica de priorização e resposta proporcional, mas não estabelece instrumento específico de maturidade em segurança da informação para EFPC. Na vertente de maturidade, Brezavšček e Baggia (2025) mostram a diversidade dos modelos existentes e destacam a necessidade de contextualização e avaliação empírica. No componente humano, Delso-Vicente *et al.* (2025) evidenciam a influência de fatores individuais e organizacionais sobre comportamentos relacionados à segurança.

No contexto financeiro brasileiro, Ferreira *et al.* (2025) acrescentam elementos relacionados à avaliação de controles cibernéticos, monitoramento e resiliência, oferecendo referência setorial complementar. Entretanto, no conjunto de fontes examinado, essas dimensões não aparecem integradas em um instrumento destinado especificamente ao contexto das EFPC e associado, de forma prospectiva, a critérios independentes de criticidade supervisória.

A contribuição do estudo organiza-se, assim, em duas camadas. No plano empírico, desenvolve e examina exploratoriamente um instrumento de maturidade em segurança da informação. No plano aplicado, propõe diretrizes para futura integração dos escores a critérios institucionais de criticidade, com finalidade de apoiar triagem e priorização. Essa segunda camada constitui proposta conceitual e não foi validada empiricamente nesta pesquisa.

Os sete domínios foram preservados como categorias teóricas e interpretativas, mesmo diante da possibilidade de a estrutura empírica revelar menor número de fatores. A Análise Fatorial Exploratória (AFE) foi utilizada justamente para investigar se essa decomposição conceitual se reproduzia nas respostas, sem pressupor previamente que os domínios correspondessem a fatores independentes.

3 METODOLOGIA

A pesquisa é aplicada, quantitativa e exploratória, realizada por levantamento survey, estratégia adequada à coleta padronizada de percepções de participantes dispersos e ao exame de associações sem pressupor causalidade (Babbie, 2010).

O percurso metodológico envolveu construção e redução do instrumento, pré-teste operacional, divulgação multicanal, depuração da base, cálculo de escores, avaliação de consistência interna, análise fatorial exploratória e exame das hipóteses. A Figura 1 resume essas etapas e separa a análise efetivamente realizada da proposta supervisória futura.

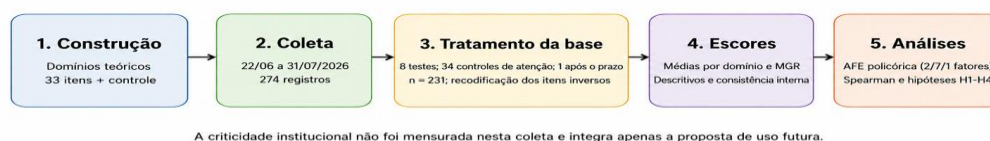


Figura 1. Percurso metodológico do estudo

Fonte: elaboração própria com base nos procedimentos descritos nesta seção.

3.1 População, amostra e cuidados éticos da coleta

O universo institucional de referência era de 264 EFPC ativas, mas a unidade de resposta foi o profissional com atuação ou experiência relacionada ao setor. A amostragem foi

não probabilística, por acessibilidade e adesão voluntária; assim, os resultados descrevem percepções dos participantes e não autorizam inferir representatividade ou maturidade das entidades.

A meta operacional foi de 150 respostas. A suficiência para AFE não depende de um limiar universal, mas da qualidade das cargas, comunalidades e estrutura obtida; a amostra final reuniu 231 respostas válidas, correspondendo a aproximadamente sete respondentes para cada um dos 33 itens submetidos à análise fatorial (MacCallum *et al.*, 1999).

A razão aproximada de sete participantes por item foi utilizada apenas como referência descritiva. A decisão sobre adequação amostral foi apoiada posteriormente pelo índice Kaiser-Meyer-Olkin (KMO), pelo teste de esfericidade de Bartlett, por medidas individuais de adequação amostral, comunalidades, cargas, análise paralela e qualidade global das soluções, evitando tratar uma razão casos/item como critério suficiente.

O formulário não solicitou nome da EFPC, Cadastro Nacional da Pessoa Jurídica (CNPJ), nome do respondente, e-mail, cidade ou outro identificador. A coleta de e-mails estava desativada, a análise foi agregada e a participação dependia de concordância voluntária, em consonância com o princípio de minimização de dados (Brasil, 2018).

Essa opção reforçou o anonimato e reduziu risco de identificação por combinação de características, mas impediu reconhecer respostas da mesma entidade, calcular cobertura institucional e realizar análises multinível. A unidade observada, portanto, permaneceu o respondente, e não a EFPC.

3.2 Instrumento e hipóteses

O questionário aplicado continha 40 itens: seis de perfil, 33 psicométricos em escala de concordância de cinco pontos e um controle de atenção. A estrutura teve como ponto de partida o questionário de Oliveira e Nunes, com adaptação ao contexto das EFPC e redução da versão ampliada de 71 para 40 itens (Oliveira; Nunes, 2025).

Os 33 itens submetidos à análise foram organizados em sete domínios teóricos: Governança e Integração (GI), Estrutura e Disciplina de Processo (EP), Sensibilidade ao Contexto (SC), Risco Cibernético e Continuidade (RC), Cultura e Engajamento em Segurança (CE), Comportamento Seguro Declarado (CS) e Maturidade Percebida (MP).

A proposta ampliada possuía 71 itens: 60 psicométricos em oito blocos, dez de perfil e um controle de atenção. A redução buscou limitar tempo de preenchimento a aproximadamente 8 a 12 minutos, reduzir fadiga e abandono e preservar anonimato. GI, EP,

SC, RC e CE foram mantidos como núcleo; CS e MP foram abreviados; o bloco de Confiança Institucional foi retirado; e o controle de atenção, CE5 e CS4 permaneceram. A rastreabilidade entre as versões é apresentada no Quadro A1 do Apêndice A.

A construção foi complementada por referências sobre governança, risco cibernético, avaliação de controles, monitoramento e resiliência no contexto financeiro brasileiro; a vinculação foi feita no nível dos domínios, e não como transcrição de escala validada (Ferreira *et al.*, 2025).

Como houve adaptação contextual, redução substancial e reescrita de itens, a versão final não herda automaticamente evidências de validade de instrumentos anteriores. A proveniência apresentada na Tabela 1 indica a principal referência de cada domínio, enquanto a validade de conteúdo permanece uma questão a aprofundar em estudos posteriores.

Tabela 1. Domínios do instrumento

Domínio	Itens	Conteúdo principal	Base principal
GI	5	Governança e integração da gestão de riscos	Oliveira e Nunes (2025)
EP	5	Formalização e disciplina dos processos	Oliveira e Nunes (2025)
SC	5	Adequação ao porte, complexidade e contexto	Oliveira e Nunes (2025)
RC	6	Risco cibernético, continuidade, terceiros e incidentes	Ferreira <i>et al.</i> (2025)
CE	5	Cultura e engajamento em segurança	Oliveira e Nunes (2025)
CS	4	Comportamento seguro declarado	Oliveira e Nunes (2025)
MP	3	Maturidade percebida	Ferreira <i>et al.</i> (2025)

Fonte: elaboração própria. ISO 31000:2018 e adaptação autoral complementaram a elaboração; a rastreabilidade detalhada da redução está no Apêndice A.

A organização preservou sete domínios teóricos com funções distintas, embora sua correspondência com dimensões empíricas independentes tenha sido posteriormente examinada pela AFE.

Antes da coleta oficial, nove pessoas participaram da etapa preparatória: autor, orientador, um colaborador do estudo e seis servidores da Previc. Oito registros foram identificados como testes; o nono foi posteriormente excluído pelo controle de atenção. Não houve alteração do instrumento após essa etapa, que é caracterizada como revisão interna e pré-teste operacional, e não como validação formal de conteúdo.

A avaliação solicitada considerava clareza, pertinência, risco de exposição ou identificação, possibilidade de interpretação sensível e adequação do tempo estimado. Como não houve protocolo padronizado de juízes, Índice de Validade de Conteúdo ou registro estruturado das avaliações, a etapa não foi usada como evidência formal de validade de conteúdo.

Os escores de GI, EP, SC e RC compuseram a Maturidade em Gestão de Riscos de Segurança da Informação (MGR), calculada pela média simples desses quatro domínios; CE, CS e MP foram analisados separadamente. H1 relacionou CE a MGR; H2, MGR a CS; H3, CE a CS; e H4, MP a GI, EP, SC, RC, CE, CS e MGR. CE5 e CS4 foram recodificados por 6 - resposta, e os escores foram calculados por médias simples, sem pesos derivados da amostra.

3.3 Coleta e tratamento dos dados

A coleta ocorreu entre 22 de junho e 31 de julho de 2026. O primeiro envio institucional foi realizado em 23 de junho para 233 endereços vinculados a EFPC, com reforço em 7 de julho. No LinkedIn, foram enviados 1.014 convites entre 24 de junho e 28 de julho, de forma progressiva em razão dos limites semanais da plataforma, além de um reforço para cada indivíduo que aceitou o convite de conexão dentro do período de pesquisa supracitado. A pesquisa também foi divulgada em um grupo de WhatsApp com 735 membros, por contatos pessoais e no blog da Associação Brasileira das Entidades Fechadas de Previdência Complementar (Abrapp). Como esses públicos podiam se sobrepor, o link era livremente compartilhável e não havia métricas completas de entrega, visualização ou clique, não foi possível determinar o número de indivíduos únicos alcançados nem calcular taxa de resposta.

Dos 274 registros, oito testes foram excluídos, 34 respostas reprovaram no controle de atenção e uma resposta foi recebida após o encerramento, resultando em 231 casos completos. Não houve imputação, ponderação por perfil ou agregação por entidade. O detalhamento do tratamento da base consta do Apêndice B.

A limpeza preservou somente casos completos e aprovados. CE5 e CS4 foram invertidos em todos os 231 registros válidos e MGR foi calculada como média de GI, EP, SC e RC. Como não havia identificador de entidade, não foram calculadas médias institucionais nem aplicadas ponderações por perfil, porte percebido ou área de atuação.

3.4 Estratégia de análise

Foram calculadas frequências, medidas descritivas, alfa de Cronbach e correlações de Spearman. Como complemento adequado à natureza ordinal dos itens, estimaram-se alfa ordinal e ômega de McDonald a partir de matrizes policóricas unifatoriais por domínio (Zumbo *et al.*, 2007).

A AFE foi executada no FACTOR 12.06.07 com matriz policórica, procedimento *Sweet Smoothing*, extração por mínimos quadrados não ponderados robustos (*Robust Unweighted Least Squares* — RULS), correção empírica LOSEFER, 500 amostras *bootstrap* e rotação oblíqua *Robust Promin*, conforme os procedimentos implementados e descritos por Lorenzo-Seva e Ferrando (2006, 2019, 2021, 2023). Foram comparadas soluções de um, dois e sete fatores, considerando análise paralela, raiz do erro quadrático médio de aproximação (RMSEA), índice de ajuste comparativo (CFI), índice de Tucker-Lewis (TLI), raiz quadrática média dos resíduos (RMSR), critério de informação bayesiano (BIC), comunalidades, cargas, correlação entre fatores, índice generalizado H de replicabilidade, confiabilidade dos escores fatoriais ORION (*Overall Reliability of fully-Informative prior Oblique N-EAP scores*), congruência unidimensional (UniCo) e variância comum explicada (ECV).

A opção pela matriz policórica decorreu da natureza ordinal dos itens. Como a matriz inicialmente estimada não era positiva definida, aplicou-se o procedimento *Sweet Smoothing* antes da extração (Lorenzo-Seva; Ferrando, 2021). A rotação oblíqua permitiu correlação entre fatores, condição coerente com a expectativa de que governança, processos, cultura e comportamento compartilhem variância.

O número de fatores foi definido prioritariamente por análise paralela com 500 matrizes aleatórias, combinada à parcimônia e à coerência teórica (Timmerman; Lorenzo-Seva, 2011). Spearman foi a análise principal das hipóteses; Pearson foi utilizado como sensibilidade. Adotou-se $p < 0,05$, sem correção por testes múltiplos, e todas as associações foram interpretadas como exploratórias.

A comparação entre um, dois e sete fatores foi deliberadamente mantida: um fator representava a hipótese de forte dimensão geral; dois fatores correspondiam à retenção indicada pela análise paralela; e sete fatores reproduziam a estrutura teórica dos domínios. A decisão final combinou retenção estatística, resíduos, parcimônia, replicabilidade e interpretabilidade, sem escolher a solução apenas pelo melhor índice de ajuste absoluto (Ferrando; Lorenzo-Seva, 2018).

3.5 Delimitação da criticidade institucional

A criticidade institucional não foi mensurada. O questionário não identificou a EFPC nem incluiu variáveis externas de exposição, materialidade ou impacto. Portanto, não foram calculados pesos, pontos de corte, níveis de criticidade ou classificação institucional. Na proposta apresentada na Seção 5, a criticidade é tratada apenas como uma dimensão a ser

obtida futuramente a partir de fontes independentes do questionário e combinada aos escores de maturidade.

Em aplicação institucional futura, essa dimensão poderia considerar porte e segmento, número de participantes e assistidos, volume de recursos administrados, sensibilidade dos dados, dependência de serviços digitais, concentração de fornecedores, relevância sistêmica e histórico de incidentes. Esses elementos não foram operacionalizados nesta pesquisa para evitar criar pesos e cortes sem validação.

3.6 Uso de inteligência artificial generativa

O ChatGPT, da OpenAI, foi utilizado como ferramenta auxiliar durante o desenvolvimento deste trabalho, principalmente na revisão linguística, reorganização e síntese de trechos, comparação entre versões do manuscrito, apoio à estruturação e revisão do instrumento de pesquisa e padronização editorial. As sugestões produzidas pela ferramenta foram avaliadas criticamente pelo autor antes de sua incorporação e não foram utilizadas como fonte primária de evidência científica nem como substitutas da literatura, da documentação oficial ou dos procedimentos estatísticos empregados no estudo.

A inteligência artificial não realizou a coleta de dados nem produziu, modificou ou completou respostas dos participantes. As decisões sobre a construção do instrumento, depuração da base, escolha dos procedimentos analíticos, interpretação dos resultados e conclusões permaneceram sob responsabilidade do autor. Informações factuais, referências e resultados associados a trechos apoiados pela ferramenta foram confrontados com as fontes originais ou com os dados efetivamente obtidos, com o objetivo de reduzir o risco de informações incorretas, referências inexistentes ou interpretações não sustentadas pelas evidências.

4 RESULTADOS

4.1 Composição da amostra

A amostra válida reuniu 231 participantes. Destes, 55,8% tinham mais de dez anos de experiência, 42,4% percebiam a EFPC como de grande porte, 95,7% informaram política de segurança formalmente aprovada e 78,4% relataram auditoria ou diagnóstico estruturado

nos dois anos anteriores. O perfil e o recrutamento voluntário recomendam cautela na generalização.

Também houve predominância de contextos percebidos como médios ou grandes e de profissionais experientes. Como a entidade não foi identificada, percentuais como porte percebido, existência de política e auditoria descrevem respostas individuais e não devem ser convertidos em proporções do universo de EFPC.

4.2 Estatísticas descritivas e consistência interna

A Tabela 2 apresenta as médias e os desvios-padrão dos domínios, juntamente com as estimativas de consistência interna obtidas pelos métodos convencional e ordinal.

Tabela 2. Estatísticas dos domínios e consistência interna

Domínio	Média	DP	α	α ord.	ω ord.
GI	4,286	0,733	0,821	0,892	0,893
EP	4,087	0,910	0,904	0,937	0,937
SC	4,267	0,757	0,853	0,910	0,910
RC	4,293	0,757	0,866	0,917	0,918
CE	4,093	0,709	0,742	0,830	0,843
CS	4,653	0,535	0,629	0,900	0,906
MP	4,398	0,690	0,796	0,887	0,893
MGR	4,233	0,695	-	-	-

Fonte: elaboração própria com dados da pesquisa (2026).

Nota: DP = desvio-padrão; α = alfa de Cronbach; α ord. = alfa ordinal; ω ord. = ômega ordinal.

As médias dos domínios ficaram acima de 4,0, com maior valor em CS e maior dispersão em EP. CS apresentou forte concentração nas categorias superiores, indicando efeito teto. Os coeficientes de consistência interna foram satisfatórios na maior parte dos domínios, mas as estimativas baseadas na matriz policórica foram sistematicamente superiores ao alfa convencional. A diferença foi particularmente pronunciada em CS, cujo α de Cronbach foi 0,629, enquanto α ordinal = 0,900 e ω ordinal = 0,906.

Essa divergência deve ser interpretada em conjunto com a distribuição das respostas. Como CS apresentou categorias pouco ou não observadas em alguns itens, os elevados coeficientes policóricos não eliminam limitações de discriminação nem tornam o domínio definitivamente validado. CS4 e o funcionamento dos itens inversos permanecem candidatos prioritários à revisão e à reaplicação em amostra independente.

4.3 Estrutura fatorial

A matriz policórica inicialmente estimada apresentou dois autovalores negativos e, portanto, não era positiva definida. O Sweet Smoothing ajustou 122 das 528 correlações únicas, com perda de 3,6% da covariância, classificada pelo FACTOR como *very good*. Após o tratamento, a matriz apresentou KMO = 0,932, teste de esfericidade de Bartlett $\chi^2(528) = 2.511,7$; $p < 0,001$ e medidas individuais de adequação amostral (MSA, do inglês *Measure of Sampling Adequacy*) superiores a 0,80 para todos os itens.

A Tabela 3 compara os principais indicadores de ajuste das soluções de um, dois e sete fatores examinadas no estudo.

Tabela 3. Comparação das soluções fatoriais

Solução	Análise Paralela	RMSEA	CFI/TLI	RMSR	BIC
1 fator	Não	0,055	0,989/0,989	0,0841	1.197,501
2 fatores	Sim	0,038	0,995/0,994	0,0594	1.159,289
7 fatores	Não	0,009	0,999/1,000	0,0272	1.761,124

Fonte: elaboração própria com dados da pesquisa e resultados do FACTOR (2026).

A análise paralela reteve dois fatores. Na análise paralela, o primeiro respondeu por 53,16% da variância considerada e reuniu principalmente GI, EP, SC e RC, sendo interpretado como capacidade institucional de gestão; o segundo respondeu por 7,41% e concentrou CE e CS, representando cultura/comportamento seguro. A correlação entre os fatores foi 0,806, indicando forte relação entre as dimensões. UniCo = 0,969 e ECV = 0,894 evidenciaram uma forte dimensão geral. A confiabilidade das estimativas dos escores fatoriais foi elevada, com ORION = 0,974 e 0,953, enquanto o H-observado = 0,891 e 0,822 indicou boa definição e potencial de replicabilidade dos dois fatores (Ferrando; Lorenzo-Seva, 2018).

A retenção do segundo fator, contudo, foi limítrofe: sua variância observada foi de 7,41%, diante de percentil 95 aleatório de 6,72%. Essa proximidade, combinada à correlação de 0,806 entre os fatores e aos índices UniCo = 0,969 e ECV = 0,894, indica que a solução bifatorial não deve ser interpretada como estrutura definitivamente estabelecida. Ao mesmo tempo, a solução unidimensional apresentou RMSR superior, enquanto a solução de sete fatores, embora produzisse melhor ajuste absoluto, não foi sustentada pela análise paralela e apresentou BIC substancialmente maior. Assim, os dois fatores constituem a hipótese estrutural mais parcimoniosa para esta amostra, em coexistência com uma forte dimensão geral.

Na matriz padrão da solução oblíqua de dois fatores, EP3, EP4 e CS3 apresentaram coeficientes superiores a 1 (1,019, 1,144 e 1,120, respectivamente). Em soluções oblíquas, coeficientes da matriz padrão não correspondem a correlações simples entre item e fator e podem ultrapassar |1|, especialmente quando os fatores são correlacionados (Watkins, 2018).

Como as comunalidades desses itens permaneceram inferiores à unidade (0,720, 0,776 e 0,661), os coeficientes superiores a 1 não foram tratados, isoladamente, como fundamento para exclusão. Ainda assim, sua ocorrência, combinada à elevada correlação entre os fatores (0,806) e à necessidade prévia de suavização da matriz policórica, recomenda cautela na interpretação da solução bifatorial (Lorenzo-Seva; Ferrando, 2021). O detalhamento das cargas e comunalidades consta do Apêndice C.

CE5 apresentou a menor comunalidade (0,216) e carga de 0,652 no segundo fator; CS4 apresentou comunalidade de 0,355 e carga de 0,819. Os dois itens foram mantidos por pertinência conceitual, mas permanecem candidatos à revisão em nova aplicação, especialmente diante do desempenho do bloco CS e do funcionamento dos itens inversos.

4.4 Associações e hipóteses

As hipóteses foram examinadas por correlação de Spearman, e a Tabela 4 apresenta os coeficientes obtidos para H1, H2, H3 e para o desdobramento de H4 em H4a–H4g.

Tabela 4. Teste exploratório das hipóteses

Hipótese	Relação	Spearman ρ	p	Resultado
H1	CE-MGR	0,578	< 0,001	Compatível com H1
H2	MGR-CS	0,368	< 0,001	Compatível com H2
H3	CE-CS	0,520	< 0,001	Compatível com H3
H4a	MP-GI	0,515	< 0,001	Compatível com H4a
H4b	MP-EP	0,652	< 0,001	Compatível com H4b
H4c	MP-SC	0,597	< 0,001	Compatível com H4c
H4d	MP-RC	0,678	< 0,001	Compatível com H4d
H4e	MP-CE	0,601	< 0,001	Compatível com H4e
H4f	MP-CS	0,385	< 0,001	Compatível com H4f
H4g	MP-MGR	0,685	< 0,001	Compatível com H4g

Fonte: elaboração própria com dados da pesquisa (2026).

Todas as associações apresentaram a direção prevista e $p < 0,001$. Como análise de sensibilidade, Pearson preservou o sinal e a significância das relações examinadas ($r = 0,407$ a $0,753$), sem alterar sua interpretação. A associação CE-CS ($\rho = 0,520$) foi numericamente superior à associação MGR-CS ($\rho = 0,368$). MP apresentou as associações mais elevadas com MGR ($\rho = 0,685$), RC ($\rho = 0,678$) e EP ($\rho = 0,652$), resultado compatível com a função sintética atribuída a MP no desenho do instrumento. Como todos os escores foram obtidos do mesmo respondente, no mesmo questionário e no mesmo momento, as associações podem estar sujeitas a efeitos de método comum (Podsakoff *et al.*, 2003). Além disso, o estudo não empregou critérios externos independentes nem desenho capaz de estabelecer causalidade; portanto, esses resultados são interpretados como coerência associativa interna entre os

escores, e não como demonstração de relação com critérios externos, causalidade ou desempenho institucional efetivo.

5 PROPOSTA DE USO SUPERVISÓRIO DO INSTRUMENTO

Esta seção apresenta uma arquitetura prospectiva de utilização dos escores produzidos pelo instrumento. A proposta articula o referencial teórico aos achados exploratórios, mas não foi aplicada a EFPC identificadas, simulada sobre a amostra nem validada como procedimento decisório. Consequentemente, as etapas e respostas descritas a seguir constituem diretrizes para avaliação futura, e não resultados empíricos desta pesquisa.

5.1 Fluxo proposto

O fluxo organiza seis etapas: coleta estruturada, validação da base, cálculo dos escores, interpretação dos escores, integração com criticidade externa e definição de resposta supervisória. A Tabela 5 sintetiza essa sequência, cuja aplicação dependeria de evidências complementares e julgamento técnico.

Tabela 5. Fluxo proposto para uso supervisório

Etapas	Descrição	Produto
1. Coleta	Aplicar o instrumento a profissionais ou unidades qualificadas	Base padronizada
2. Validação	Tratar respostas e itens reversos	Base válida
3. Escores	Calcular domínios e MGR	Perfil de escores
4. Interpretação	Analisar escores contínuos	Interpretação dos escores
5. Criticidade	Combinar com critérios institucionais externos	Matriz maturidade-criticidade
6. Resposta	Definir medida proporcional	Plano supervisório

Fonte: elaboração própria com base em IOPS (2023).

O fluxo admite duas finalidades distintas. Em aplicações anônimas, o instrumento pode produzir diagnóstico agregado sobre percepções de maturidade no setor. Uma aplicação institucional identificada, entretanto, exigiria desenho próprio, preferencialmente com múltiplos informantes por entidade, regra de agregação, tratamento das divergências entre respondentes, controle de acesso e triangulação com documentos, incidentes, auditorias e outras evidências. Assim, a passagem do diagnóstico individual para uma interpretação institucional não é automática.

5.2 Integração prospectiva entre maturidade e criticidade

A MGR corresponde à média de GI, EP, SC e RC; CE e CS qualificam a dimensão cultural-comportamental, e MP constitui medida sintética complementar. Os escores permanecem na escala original de 1 a 5 e devem ser interpretados prioritariamente como variáveis contínuas.

A criticidade institucional constitui dimensão distinta da maturidade e deverá ser determinada por metodologia externa ao instrumento. Entre as variáveis potencialmente relevantes estão porte e segmento, número de participantes e assistidos, volume de recursos administrados, sensibilidade dos dados, dependência de serviços digitais, concentração de fornecedores, relevância sistêmica e histórico de incidentes. Esta pesquisa não definiu pesos, pontos de corte ou regras de classificação para essa dimensão (IOPS, 2023).

Em eventual aplicação futura, maturidade e criticidade poderiam ser consideradas conjuntamente para orientar a intensidade da resposta supervisória. A Tabela 6 apresenta essa relação exclusivamente como representação conceitual, destinada a demonstrar a lógica de proporcionalidade e não a estabelecer uma regra decisória.

Tabela 6. Matriz ilustrativa de maturidade e criticidade

Maturidade em Segurança da Informação	Criticidade baixa	Criticidade média	Criticidade alta
Menor maturidade	Acompanhamento orientativo	Diligência ou supervisão temática	Fiscalização prioritária
Maturidade intermediária	Monitoramento ordinário	Monitoramento com recomendações	Supervisão temática
Maior maturidade	Monitoramento periódico	Monitoramento periódico	Monitoramento com validação pontual

Fonte: elaboração própria com base em IOPS (2023).

Nota: as categorias são exclusivamente ilustrativas. O estudo não definiu pesos, pontos de corte ou regras de classificação da maturidade ou da criticidade das EFPC, e a matriz não foi aplicada nem validada empiricamente.

A matriz expressa dois princípios da supervisão baseada em risco: maior maturidade percebida não elimina a necessidade de atenção quando a criticidade institucional é elevada, e menor criticidade não neutraliza fragilidades relevantes de segurança da informação. Em aplicação real, a resposta dependeria dos escores, da criticidade externa, das evidências disponíveis e do julgamento técnico supervisor (IOPS, 2023). A matriz, portanto, organiza possibilidades de atuação, mas não produz decisão automática.

5.3 Acompanhamento e limites de uso

A reaplicação periódica do instrumento poderia permitir o acompanhamento de tendências, recorrência de fragilidades e evolução dos escores. Essa utilização produziria avaliações sucessivas em momentos distintos, e não monitoramento contínuo de segurança da informação, que envolve visibilidade recorrente sobre ativos, ameaças, vulnerabilidades e efetividade de controles (Dempsey *et al.*, 2011). Como a pesquisa foi transversal, não foram avaliadas estabilidade temporal, sensibilidade à mudança ou capacidade de antecipar incidentes; esses atributos precisariam ser examinados em aplicações sucessivas antes de qualquer interpretação longitudinal.

O instrumento também deve ser tratado como mecanismo de triagem e apoio à análise, e não como substituto de auditorias ou verificações técnicas. Autorrelato, conhecimento parcial da organização e efeito teto recomendam cautela; além disso, a desejabilidade social pode favorecer respostas excessivamente positivas (Zaal *et al.*, 2026). Por isso, resultados positivos não dispensariam validação por outras evidências, enquanto resultados desfavoráveis não poderiam fundamentar automaticamente medidas supervisoras ou sancionatórias.

A natureza da fragilidade também deve orientar a resposta. Escores relativamente baixos em governança ou processos demandariam evidências diferentes daquelas relacionadas a risco cibernético ou cultura de segurança. Essa diferenciação preserva a proporcionalidade e evita converter uma pontuação agregada em resposta fiscalizatória padronizada.

6 DISCUSSÃO

6.1 Estrutura interna, consistência e relações entre os domínios

Os resultados indicam que os sete domínios definidos teoricamente não se reproduziram como sete dimensões empíricas independentes. GI, EP, SC e RC apresentaram predominância na dimensão associada à capacidade institucional de gestão, enquanto CE e CS se concentraram na dimensão cultural-comportamental. Essa organização é conceitualmente plausível porque governança, processos, gestão do risco cibernético e fatores humanos constituem componentes relacionados de uma mesma capacidade organizacional de segurança, ainda que possam ser examinados separadamente para fins diagnósticos (NIST, 2024).

A interpretação da dimensionalidade, entretanto, requer cautela. A análise paralela reteve dois fatores, mas o segundo componente superou por margem relativamente pequena o percentil 95 das matrizes aleatórias. Além disso, a correlação de 0,806 entre os fatores, associada a $UniCo = 0,969$ e $ECV = 0,894$, indica presença de forte dimensão geral. A solução de um fator também apresentou bons índices de ajuste, embora com resíduos superiores, enquanto sete fatores melhoraram o ajuste absoluto sem respaldo da análise paralela e com BIC substancialmente maior. O conjunto das evidências favorece, portanto, uma hipótese exploratória de dois fatores correlacionados coexistindo com uma dimensão geral forte, e não uma estrutura definitiva.

Essa constatação também delimita a interpretação dos escores. Os sete domínios permanecem úteis como categorias teóricas para localizar diferentes aspectos das respostas, mas os resultados desta amostra não demonstram que cada domínio corresponda a um fator latente independente. Da mesma forma, a MGR deve ser entendida como indicador composto definido teoricamente pela média de GI, EP, SC e RC, e não como escore fatorial empiricamente validado. Essa distinção é relevante porque modelos de maturidade ganham utilidade quando preservam a interpretabilidade dos resultados sem transformar categorias conceituais em faixas ou níveis de maturidade não demonstrados empiricamente (Brezavšček; Baggia, 2025).

A consistência interna apresentou outro resultado que merece interpretação. GI, EP, SC, RC, CE e MP apresentaram coeficientes satisfatórios, enquanto CS registrou α de Cronbach = 0,629. Entretanto, para esse mesmo domínio, α ordinal = 0,900 e ω ordinal = 0,906. Estimativas ordinais podem ser mais apropriadas para itens Likert quando calculadas a partir de correlações policóricas, mas valores elevados não devem ser interpretados isoladamente quando a distribuição contém efeito teto e categorias pouco observadas (Zumbo *et al.*, 2007). No presente estudo, a discrepância entre os coeficientes, somada ao aumento do alfa convencional após a retirada de CS4, indica a necessidade de revisar o domínio em nova aplicação, especialmente o funcionamento do item inverso.

As associações previstas também apresentaram direção coerente com as hipóteses. Cultura e engajamento relacionaram-se positivamente à MGR e ao comportamento seguro declarado, enquanto a maturidade percebida apresentou associações positivas com todos os demais domínios. A relação CE-CS foi mais elevada que MGR-CS, sugerindo maior proximidade entre comportamento declarado e características culturais percebidas do que entre comportamento e estrutura formal de gestão. Esse padrão é compatível com a literatura

que atribui papel conjunto a fatores individuais e organizacionais na conformidade em segurança da informação (Delso-Vicente *et al.*, 2025).

Essas correlações, contudo, não demonstram relação com critérios externos independentes nem causalidade. Todos os escores foram obtidos do mesmo respondente, no mesmo questionário e no mesmo momento, condição que pode introduzir efeitos de método comum (Podsakoff *et al.*, 2003). Assim, uma percepção globalmente favorável da organização pode elevar simultaneamente respostas sobre governança, processos, cultura e comportamento. Os resultados demonstram coerência associativa interna do instrumento nesta amostra e fornecem hipóteses para estudos subsequentes, mas precisam ser confrontados com critérios independentes.

6.2 Implicações projetadas para supervisão

Os resultados permitem discutir o instrumento como mecanismo exploratório de organização de sinais, mas não como classificador de EFPC. Em uma aplicação futura, a MGR poderia oferecer síntese das percepções relacionadas à capacidade de gestão, enquanto os domínios permitiriam localizar fragilidades específicas e CE e CS acrescentariam informação sobre a dimensão cultural-comportamental. A prioridade supervisória dependeria ainda de uma medida de criticidade construída com informações externas ao questionário, preservando a lógica de proporcionalidade própria da supervisão baseada em risco (IOPS, 2023).

As médias elevadas observadas nesta pesquisa não autorizam concluir que o setor apresente baixa exposição cibernética ou maturidade institucional elevada. A amostragem voluntária, o recrutamento aberto, o predomínio de profissionais experientes e a própria natureza do autorrelato podem ter favorecido respostas mais positivas. Além disso, o participante pode conhecer bem determinada área e apenas parcialmente outras práticas da organização. A deseabilidade social constitui limitação conhecida em levantamentos que envolvem comportamentos considerados normativamente desejáveis (Zaal *et al.*, 2026).

Por essas razões, uma transição para uso supervisório deveria ocorrer por etapas. Uma primeira reaplicação poderia verificar estabilidade dos itens, funcionamento das categorias de resposta e replicação da estrutura interna. Posteriormente, um piloto identificado poderia utilizar múltiplos informantes por EFPC e comparar os escores agregados com evidências externas, como auditorias, incidentes, registros de continuidade, informações sobre

terceiros e achados de supervisão. Somente depois dessa etapa seria possível investigar se os escores acrescentam informação útil à priorização realizada pelo supervisor.

A reaplicação periódica também deve ser distinguida de monitoramento contínuo de segurança da informação (Dempsey *et al.*, 2011). O estudo atual é transversal e não avaliou sensibilidade à mudança, estabilidade temporal, capacidade preditiva ou antecipação de incidentes. Consequentemente, acompanhar a evolução dos escores constitui possibilidade a ser testada, e não funcionalidade demonstrada pelo estudo. Essa delimitação evita atribuir ao instrumento capacidades próprias de monitoramento técnico de eventos ou controles que ele não foi projetado para substituir.

6.3 Limitações e agenda de pesquisa

A primeira limitação decorre da amostragem não probabilística e do recrutamento voluntário. Como não foi possível determinar o número de indivíduos únicos alcançados nem identificar as EFPC representadas, não se puderam calcular taxa de resposta, estimar viés de não resposta ou avaliar cobertura institucional. Também não é possível excluir a participação de múltiplos profissionais de uma mesma entidade. Assim, os resultados descrevem os 231 respondentes e não podem ser interpretados como estimativa da distribuição de maturidade das EFPC brasileiras.

A segunda limitação está relacionada à mensuração. O instrumento utiliza autorrelato e todas as variáveis foram coletadas na mesma ocasião, o que favorece interpretação heterogênea, desejabilidade social e viés de método comum. Essas condições são particularmente relevantes para as hipóteses associativas, pois uma tendência geral de avaliação positiva pode aumentar simultaneamente diferentes escores (Podsakoff *et al.*, 2003). A desejabilidade social constitui limitação adicional em levantamentos sobre comportamentos normativamente desejáveis (Zaal *et al.*, 2026). O desenho transversal também impede inferências causais e avaliação de evolução temporal (Babbie, 2010).

No plano psicométrico, a AFE foi realizada na mesma amostra empregada no desenvolvimento inicial do instrumento. A matriz policórica necessitou de Sweet Smoothing, alguns itens apresentaram forte assimetria, efeito teto ou categorias esparsas e três coeficientes da matriz padrão ultrapassaram a unidade. Embora essas ocorrências não tenham determinado exclusão automática de itens, reforçam a necessidade de replicação. A solução de dois fatores deve ser tratada como hipótese estrutural e não como arquitetura consolidada.

A evidência de conteúdo também permanece inicial. A construção combinou literatura, discussão entre os pesquisadores e pré-teste operacional, mas não houve protocolo formal de avaliação independente por juízes. Da mesma forma, a criticidade institucional não foi mensurada, e a matriz maturidade $\times$ criticidade não foi aplicada às respostas nem validada empiricamente. Esses elementos pertencem à etapa prospectiva da pesquisa.

Como agenda, recomenda-se revisar CS4 e itens com menor desempenho, realizar nova avaliação de conteúdo por especialistas independentes, reaplicar o instrumento em amostra distinta e posteriormente testar sua estrutura por análise fatorial confirmatória. Havendo amostra suficiente e identificação institucional apropriada, poderão ser examinadas invariância entre grupos, concordância entre múltiplos informantes da EFPC, estabilidade temporal e relação com critérios externos. Em paralelo, a metodologia de criticidade e eventuais regras de decisão supervisória deverão ser desenvolvidas e validadas separadamente antes de qualquer aplicação individualizada.

7 CONCLUSÃO

O estudo desenvolveu um instrumento de maturidade em segurança da informação adaptado ao contexto das Entidades Fechadas de Previdência Complementar e examinou exploratoriamente sua estrutura interna, consistência e relações entre os domínios propostos. A análise das 231 respostas válidas mostrou médias elevadas nos escores, associações positivas nas relações hipotetizadas e evidência de uma estrutura mais agregada que os sete domínios teóricos originalmente definidos.

A análise fatorial indicou dois fatores correlacionados, associados predominantemente à capacidade institucional de gestão e à cultura e ao comportamento seguro, coexistindo com uma forte dimensão geral. Essa configuração deve ser interpretada como hipótese estrutural para replicação, e não como solução definitiva. Os sete domínios permanecem úteis como categorias teóricas e interpretativas, enquanto a MGR constitui indicador composto definido conceitualmente pela média de GI, EP, SC e RC. O domínio de comportamento seguro e, em particular, o funcionamento dos itens inversos requerem aperfeiçoamento em novas aplicações.

Em resposta ao problema de pesquisa, os resultados indicam que é possível estruturar um instrumento capaz de produzir sinais padronizados sobre percepções relacionadas à maturidade em segurança da informação no contexto estudado. Entretanto, os dados desta

pesquisa não permitem converter esses sinais diretamente em avaliação da maturidade de uma EFPC específica. A unidade observada foi o profissional respondente, a coleta foi anônima e não houve identificação das entidades, mensuração de criticidade institucional ou comparação dos escores com critérios externos de desempenho.

A utilização em supervisão baseada em risco constitui, portanto, uma segunda camada da proposta. Em aplicação futura, os escores poderão ser combinados com critérios independentes de criticidade e com evidências institucionais para apoiar triagem, priorização e definição proporcional da intensidade supervisória. A matriz maturidade $\times$ criticidade apresentada no estudo representa apenas essa lógica conceitual; não estabelece pesos, pontos de corte ou regras decisórias e não foi validada empiricamente.

O avanço para uso institucional requer nova avaliação do instrumento em amostra independente, aprimoramento dos itens com menor desempenho, avaliação formal de conteúdo, análise confirmatória, múltiplos informantes por entidade e comparação com auditorias, incidentes e outras evidências externas. Um piloto posterior poderá então examinar estabilidade, utilidade decisória, custos e governança da aplicação. Até que essas etapas sejam cumpridas, os escores devem ser tratados como sinais exploratórios de apoio à análise, e não como certificação, ranking, classificação de EFPC ou fundamento automático para medidas supervisoras ou sancionatórias.

REFERÊNCIAS

BABBIE, Earl. *The practice of social research*. 12. ed. Belmont: Wadsworth, 2010.

BB PREVIDÊNCIA. Fato relevante – exposição de dados. 8 maio 2020. Disponível em: <https://bbprevidencia.com.br/blog/fato-relevante-vazamento-de-informacoes/>. Acesso em: 18 ago. 2026.

BRASIL. Lei nº 12.154, de 23 de dezembro de 2009. Cria a Superintendência Nacional de Previdência Complementar – PREVIC e dispõe sobre outras matérias relativas ao regime de previdência complementar. Diário Oficial da União: seção 1, edição extra, Brasília, DF, 23 dez. 2009. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2007-2010/2009/lei/112154.htm. Acesso em: 18 ago. 2026.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais. Diário Oficial da União: seção 1, Brasília, DF, 15 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709compilado.htm. Acesso em: 30 jul. 2026.

BRASIL. Superintendência Nacional de Previdência Complementar. Portaria PREVIC nº 539, de 17 de junho de 2025. Atualiza a segmentação das entidades fechadas de previdência complementar — EFPC para fins de supervisão, fiscalização e proporcionalidade normativa para o ano de 2026. Diário Oficial da União: seção 1, Brasília, DF, 23 jun. 2025, p. 62. Disponível em: <https://www.gov.br/previc/pt-br/aceso-a-informacao-1/institucional/normas/processo-normativo-air-arr-e-consultas-publicas/air/nao-aplicabilidade-ou-dispensas-de-air-1/portaria-previc-no-539-de-17-de-junho-de-2025>. Acesso em: 26 ago. 2026.

BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos. Secretaria de Governo Digital. Guia do Framework de Privacidade e Segurança da Informação: PPSI 2.0. Versão 1.2. Brasília, DF: MGI, 2026a. Disponível em: <https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi-2.0/arquivos/guiafwppsi2-0-v1-2-11062026.pdf>. Acesso em: 30 jul. 2026.

BRASIL. Superintendência Nacional de Previdência Complementar. Painel PREVIC - Cidadão. Brasília, DF: Previc, 2026b. Disponível em: <https://www.gov.br/previc/pt-br/aceso-a-informacao-1/painel-previc/painel-previc>. Acesso em: 11 jun. 2026.

BRASIL. Superintendência Nacional de Previdência Complementar. PREVIC define procedimentos de fiscalização em 111 fundos de pensão em 2026. Brasília, DF: Previc, 6 jan. 2026c. Disponível em: <https://www.gov.br/previc/pt-br/noticias/previc-define-procedimentos-de-fiscalizacao-em-111-fundos-de-pensao-em-2026>. Acesso em: 18 ago. 2026.

BRASIL. Superintendência Nacional de Previdência Complementar. Relatório 2025 da Previdência Complementar Fechada. Brasília, DF: Previc, 2026d. Disponível em: <https://www.gov.br/previc/pt-br/publicacoes/relatorio-de-estabilidade-da-previdencia-complementar-rep/relatorio-2025-de-previdencia-complementar-julho-2026/%40%40display-file/file>. Acesso em: 17 ago. 2026.

BREZAVŠČEK, Alenka; BAGGIA, Alenka. Recent trends in information and cyber security maturity assessment: a systematic literature review. *Systems*, v. 13, n. 1, artigo 52, 2025. Disponível em: <https://doi.org/10.3390/systems13010052>. Acesso em: 30 jul. 2026.

DELISO-VICENTE, Alberto-Tomas; DIAZ-MARCOS, Luis; AGUADO-TEVAR, Oscar; GARCÍA DE BLANES-SEBASTIÁN, María. Factors influencing employee compliance with information security policies: a systematic literature review of behavioral and technological aspects in cybersecurity. *Future Business Journal*, v. 11, artigo 28, 2025. Disponível em: <https://doi.org/10.1186/s43093-025-00452-7>. Acesso em: 4 ago. 2026.

DEMPSEY, Kelley L.; JOHNSON, L. A.; SCHOLL, Matthew A.; STINE, Kevin M.; JONES, Alicia Clay; OREBAUGH, Angela; CHAWLA, Nirali S.; JOHNSTON, Ronald. Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations. NIST Special Publication 800-137. Gaithersburg, MD: National Institute of Standards and Technology, 2011. Disponível em: <https://doi.org/10.6028/NIST.SP.800-137>. Acesso em: 26 ago. 2026.

FERRANDO, Pere J.; LORENZO-SEVA, Urbano. Assessing the quality and appropriateness of factor solutions and factor score estimates in exploratory item factor analysis. *Educational and Psychological Measurement*, v. 78, n. 5, p. 762-780, 2018. Disponível em: <https://doi.org/10.1177/0013164417719308>. Acesso em: 3 ago. 2026.

FERREIRA, Lucas Vinicius Andrade; ALVES, Carlos André de Melo; MELO, Laerte Peotta de; NUNES, Rafael Rabelo. Internal Audit Strategies for Assessing Cybersecurity Controls in the Brazilian Financial Institutions. *Applied Sciences*, v. 15, n. 10, art. 5715, 2025. Disponível em: <https://doi.org/10.3390/app15105715>. Acesso em: 15 ago. 2026.

HERATH, Tejaswini; RAO, H. Raghav. Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of Information Systems*, v. 18, n. 2, p. 106-125, 2009. Disponível em: <https://doi.org/10.1057/ejis.2009.6>. Acesso em: 30 jul. 2026.

INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA (IBGE). PIB cresce 2,3% em 2025 e fecha o ano em R\$ 12,7 trilhões. Agência de Notícias IBGE, 3 mar. 2026. Disponível em: <https://agenciadenoticias.ibge.gov.br/agencia-sala-de-imprensa/2013-agencia-de->

[noticias/releases/45968-pib-cresce-2-3-em-2025-e-fecha-o-ano-em-r-12-7-trilhoes](#). Acesso em: 18 ago. 2026.

INTERNATIONAL ORGANISATION OF PENSION SUPERVISORS. Supervisory approaches to enhancing cyber resilience in the private pension sector: high-level summary of members responses to the questionnaire. *IOPS Working Papers on Effective Pensions Supervision*, n. 37, Paris, 2021. Disponível em: <https://www.oecd.org/content/dam/iops/en/working-papers/WP-37-IOPS-Supervisory-Approaches-Enhancing-Cyber-Resilience.pdf>. Acesso em: 30 jul. 2026.

INTERNATIONAL ORGANISATION OF PENSION SUPERVISORS. Introduction to the IOPS Risk-Based Supervision Toolkit. Public version. Paris: IOPS, 2023. Disponível em: https://www.iopsweb.org/content/dam/iops/en/rbs-toolkit/Module_0_-_IOPS_RBS_Toolkit.pdf. Acesso em: 30 jul. 2026.

ISO. ISO 31000:2018: Risk management - Guidelines. Geneva: International Organization for Standardization, 2018. Disponível em: <https://www.iso.org/standard/65694.html>. Acesso em: 26 ago. 2026.

ISO. ISO/IEC 27001:2022: Information security, cybersecurity and privacy protection - Information security management systems - Requirements. Geneva: International Organization for Standardization, 2022. Disponível em: <https://www.iso.org/standard/27001.html>. Acesso em: 30 jul. 2026.

LORENZO-SEVA, Urbano; FERRANDO, Pere J. FACTOR: a computer program to fit the exploratory factor analysis model. *Behavior Research Methods*, v. 38, n. 1, p. 88-91, 2006. Disponível em: <https://doi.org/10.3758/BF03192753>. Acesso em: 30 jul. 2026.

LORENZO-SEVA, Urbano; FERRANDO, Pere J. Robust Promin: a method for diagonally weighted factor rotation. *Liberabit*, v. 25, n. 1, p. 99-106, 2019. Disponível em: <https://doi.org/10.24265/liberabit.2019.v25n1.08>. Acesso em: 30 jul. 2026.

LORENZO-SEVA, Urbano; FERRANDO, Pere J. Not positive definite correlation matrices in exploratory item factor analysis: causes, consequences and a proposed solution. *Structural Equation Modeling: A Multidisciplinary Journal*, v. 28, n. 1, p. 138-147, 2021. Disponível em: <https://doi.org/10.1080/10705511.2020.1735393>. Acesso em: 30 jul. 2026.

LORENZO-SEVA, Urbano; FERRANDO, Pere J. A simulation-based scaled test statistic for assessing model-data fit in least-squares unrestricted factor-analysis solutions. *Methodology*, v. 19, p. 96-115, 2023. Disponível em: <https://doi.org/10.5964/meth.9839>. Acesso em: 30 jul. 2026.

MACCALLUM, Robert C.; WIDAMAN, Keith F.; ZHANG, Shaobo; HONG, Sehee. Sample size in factor analysis. *Psychological Methods*, v. 4, n. 1, p. 84-99, 1999. Disponível em: <https://doi.org/10.1037/1082-989X.4.1.84>. Acesso em: 30 jul. 2026.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. The NIST Cybersecurity Framework (CSF) 2.0. Gaithersburg, MD: NIST, 2024. Disponível em: <https://doi.org/10.6028/NIST.CSWP.29>. Acesso em: 30 jul. 2026.

OLIVEIRA, Patrícia Araújo de; NUNES, Rafael Rabelo. Levantamento da percepção dos princípios da ISO 31000:2018 para proposição de medidas de controle de gestão de riscos de segurança da informação no setor público. 2025. Trabalho de Conclusão de Curso (Especialização em Privacidade e Segurança da Informação) - Programa de Pós-Graduação em Engenharia Elétrica, Universidade de Brasília, Brasília, DF, 2025.

PODSAKOFF, Philip M.; MACKENZIE, Scott B.; LEE, Jeong-Yeon; PODSAKOFF, Nathan P. Common method biases in behavioral research: a critical review of the literature and recommended remedies. *Journal of Applied Psychology*, v. 88, n. 5, p. 879-903, 2003. Disponível em: <https://doi.org/10.1037/0021-9010.88.5.879>. Acesso em: 26 ago. 2026.

TIMMERMAN, Marieke E.; LORENZO-SEVA, Urbano. Dimensionality assessment of ordered polytomous items with parallel analysis. *Psychological Methods*, v. 16, n. 2, p. 209-220, 2011. Disponível em: <https://doi.org/10.1037/a0023353>. Acesso em: 30 jul. 2026.

UCHENDU, Betsy; NURSE, Jason R. C.; BADA, Maria; FURNELL, Steven. Developing a cyber security culture: current practices and future needs. *Computers & Security*, v. 109, artigo 102387, 2021. Disponível em: <https://doi.org/10.1016/j.cose.2021.102387>. Acesso em: 4 ago. 2026.

WATKINS, Marley W. Exploratory factor analysis: a guide to best practice. *Journal of Black Psychology*, v. 44, n. 3, p. 219-246, 2018. Disponível em: <https://doi.org/10.1177/0095798418771807>. Acesso em: 26 ago. 2026.

ZAAL, Emma; ONGENA, Yfke; VAN DER VELDEN, Nina; LOUGHNAN, Dan; HOEKS, John. Unraveling honest responding: a systematic review on the effectiveness of social desirability bias reduction methods in survey research. *Quality & Quantity*, v. 60, p. 10359-10391, 2026. Disponível em: <https://doi.org/10.1007/s11135-026-02664-7>. Acesso em: 4 ago. 2026.

ZUMBO, Bruno D.; GADERMANN, Anne M.; ZEISSER, Cornelia. Ordinal versions of coefficients alpha and theta for Likert rating scales. *Journal of Modern Applied Statistical Methods*, v. 6, n. 1, p. 21-29, 2007. Disponível em: <https://doi.org/10.22237/jmasm/1177992180>. Acesso em: 17 ago. 2026.

APÊNDICE A — RASTREABILIDADE DA REDUÇÃO DO INSTRUMENTO

O Quadro A1 sintetiza a correspondência entre a proposta ampliada de 71 itens e a versão efetivamente aplicada, evidenciando retenções, exclusões, renumerações e consolidações.

Quadro A1. Rastreabilidade documental da redução da proposta de 71 itens para a versão aplicada

Bloco	Itens	Correspondência entre a proposta de 71 itens e a versão aplicada
Perfil	10 para 6	PR1-PR4 foram mantidos com ajustes de alternativas; PR7 passou a PR5 e PR8 passou a PR6. PR5, PR6, PR9 e PR10 da proposta não aparecem na versão aplicada.
GI	6 para 5	GI1-GI5 foram mantidos com adaptações de redação. GI6 da proposta não aparece na versão aplicada.
EP	6 para 5	EP1-EP4 foram mantidos com adaptações; EP6 passou a EP5. EP5 da proposta não aparece na versão aplicada.
SC	6 para 5	SC1-SC3 foram mantidos; SC5 passou a SC4 e SC6 passou a SC5. SC4 da proposta não aparece na versão aplicada.
RC	6 para 6	RC1-RC6 foram mantidos, com ajustes de redação voltados a ameaças, continuidade, incidentes, terceiros e dados pessoais no contexto das EFPC.
CE	6 para 5	CE1-CE4 foram mantidos; CE6, item inverso, passou a CE5. CE5 da proposta não aparece na versão aplicada.
CS	6 para 4	CS1 foi mantido; CS3 passou a CS2, CS4 passou a CS3 e CS6, item inverso, passou a CS4. CS2 e CS5 da proposta não aparecem na versão aplicada.
CI	5 para 0	O bloco autônomo de Confiança Institucional foi retirado para reduzir extensão e complexidade do modelo.
MP	5 para 3	Os cinco itens foram consolidados e reescritos em três itens globais de percepção de estruturação, preparo e evolução. A correspondência é conceitual, e não item a item.
AC	1 para 1	O controle de atenção foi mantido; a redação final foi ajustada ao rótulo da alternativa 4 da escala aplicada.
Total	71 para 40	A redução resultou em 60 para 33 itens psicométricos, 10 para 6 itens de perfil e manutenção de um controle de atenção.

Fonte: comparação entre a proposta ampliada fornecida pelo autor, a versão final do formulário e o histórico de preparação recuperado.

A comparação permite identificar retenções, exclusões, renumerações e consolidações. Entretanto, não foi localizado registro contemporâneo que justificasse individualmente cada exclusão ou reescrita; por isso, o quadro não deve ser interpretado como evidência, por si só, de validade de conteúdo nem como comprovação de cobertura exaustiva dos oito princípios da ISO 31000:2018 pela versão final.

APÊNDICE B — TRATAMENTO E COMPOSIÇÃO DA BASE DE DADOS

Este apêndice detalha a formação da amostra final, o perfil agregado dos participantes e os procedimentos aplicados à base antes das análises.

Os registros disponíveis de recrutamento confirmam 233 envios a endereços vinculados a EFPC, com disparos em 23 de junho e 7 de julho de 2026; 1.014 convites diretos pelo LinkedIn entre 24 de junho e 28 de julho, com um reforço sem data exata registrada; divulgação em um grupo de WhatsApp com 735 membros; contatos pessoais; e publicação no blog da Abrapp. O encaminhamento livre, a sobreposição de públicos e a inexistência de métricas de alcance impedem estabelecer denominador único e calcular taxa de resposta.

A Tabela B1 apresenta a depuração dos 274 registros recebidos.

Tabela B1. Controle inicial das respostas

Indicador	Quantidade	Percentual
Registros recebidos	274	100,0%
Respostas de teste excluídas	8	2,9%
Registros submetidos ao controle de atenção	265	96,7%
Excluídas pelo controle de atenção	34	12,4% dos registros; 12,8% dos registros submetidos ao controle de atenção
Resposta posterior ao encerramento	1	0,4%; separada da análise
Respostas válidas	231	84,3% dos registros; 87,2% dos registros submetidos ao controle de atenção

Fonte: elaboração própria com dados da pesquisa (2026).

Após a exclusão dos oito registros identificados especificamente como testes e da resposta posterior ao encerramento, 265 registros foram considerados para aplicação do critério de controle de atenção. Desses, 34 foram reprovados, incluindo o registro do nono participante da etapa preparatória, resultando em 231 casos válidos.

A Tabela B2 resume o perfil dos participantes, sem inferir representatividade das EFPC.

Tabela B2. Perfil agregado dos respondentes

Variável de perfil	Categoria predominante	Percentual	Observação
Área de atuação	Área operacional, benefícios, atendimento ou investimentos	40,3%	93 respondentes; TI/segurança da informação representou 16,9%.
Tempo de experiência	Mais de 10 anos	55,8%	75,3% possuíam seis anos ou mais.
Porte percebido da EFPC	Grande porte	42,4%	Médio porte apresentou 41,6%.
Terceirização de TI/segurança da informação	Médio	43,3%	Alto: 29,4%; baixo: 27,3%.

Variável de perfil	Categoria predominante	Percentual	Observação
Política de SI formalmente aprovada	Sim	95,7%	221 respondentes.
Auditoria ou diagnóstico nos últimos dois anos	Sim	78,4%	181 respondentes.

Fonte: elaboração própria com dados da pesquisa (2026).

A predominância de profissionais experientes e de contextos percebidos como médios ou grandes recomenda cautela na interpretação das médias elevadas.

A Tabela B3 registra as exclusões e recodificações aplicadas antes das análises.

Tabela B3. Procedimentos de tratamento da base

Procedimento	Critério	Quantidade afetada
Exclusão de registros de teste	Registro anterior a 22/06/2026, confirmado como teste	8
Exclusão de respostas incompletas	Resposta parcial ou ausente	0
Exclusão pelo controle de atenção	AC1 diferente de “Concordo parcialmente”	34
Separação após o encerramento	Registro recebido em 01/08/2026	1
Recodificação de CE5	Valor invertido = 6 - resposta original	231
Recodificação de CS4	Valor invertido = 6 - resposta original	231

Fonte: elaboração própria com dados da pesquisa (2026).

Não houve imputação, ponderação nem agregação por entidade; CE5 e CS4 foram invertidos em todos os 231 casos válidos.

APÊNDICE C — RESULTADOS ANALÍTICOS DETALHADOS

Este apêndice reúne estatísticas descritivas, consistência interna, adequação fatorial, cargas dos itens, comparação entre soluções e associações exploratórias.

A Tabela C1 detalha a distribuição dos escores por domínio.

Tabela C1. Estatísticas descritivas dos domínios

Domínio	Média	Mediana	Desvio-padrão	Mínimo	Máximo	Interpretação preliminar
GI - Governança e Integração	4,286	4,400	0,733	1,400	5,000	Média e mediana superiores a 4
EP - Estrutura e Disciplina de Processo	4,087	4,400	0,910	1,000	5,000	Menor média entre os domínios de MGR; maior dispersão
SC - Sensibilidade ao Contexto	4,267	4,400	0,757	1,200	5,000	Média e mediana superiores a 4
RC - Risco Cibernético e Continuidade	4,293	4,500	0,757	1,500	5,000	Maior média entre os domínios de MGR
CE - Cultura e Engajamento em Segurança	4,093	4,200	0,709	1,800	5,000	Menor média entre CE e CS
CS - Comportamento Seguro Declarado	4,653	5,000	0,535	1,750	5,000	Maior média geral; efeito teto
MP - Maturidade Percebida	4,398	4,667	0,690	2,000	5,000	Média e mediana superiores a 4

Fonte: elaboração própria com dados da pesquisa (2026).

Os escores foram concentrados na parte superior da escala, com maior dispersão em EP e efeito teto mais pronunciado em CS. As interpretações da última coluna são descritivas e não validam níveis de maturidade.

A Tabela C2 apresenta as estimativas de consistência interna de cada domínio.

Tabela C2. Consistência interna dos domínios

Domínio	Nº de itens	Alfa de Cronbach	α ordinal	ω ordinal	Interpretação	Observação
GI	5	0,821	0,892	0,893	Bom	-
EP	5	0,904	0,937	0,937	Elevado	-
SC	5	0,853	0,910	0,910	Bom	-
RC	6	0,866	0,917	0,918	Bom	-
CE	5	0,742	0,830	0,843	Adequado	-
CS	4	0,629	0,900	0,906	Aceitável com cautela	Sem CS4: $\alpha = 0,856$; item mantido.
MP	3	0,796	0,887	0,893	Adequado	-

Fonte: elaboração própria com dados da pesquisa (2026).

CS apresentou o menor alfa e forte sensibilidade à retirada de CS4. As estimativas ordinais foram superiores aos respectivos alfas convencionais. A diferença foi especialmente acentuada em CS ($\alpha = 0,629$; α ordinal = 0,900; ω ordinal = 0,906), domínio que também

apresentou forte efeito teto e categorias de resposta esparsas. Por essa razão, a elevada confiabilidade estimada no modelo ordinal deve ser interpretada conjuntamente com a distribuição empírica dos itens e não elimina a recomendação de revisão e reaplicação do bloco.

A Tabela C3 reúne a adequação da matriz e a retenção dimensional.

Tabela C3. Adequação da matriz e retenção dimensional

Indicador	Resultado	Interpretação
KMO geral	0,932	Muito bom
Bartlett	$\chi^2(528) = 2.511,7; p < 0,001$	Matriz fatorável
MSA individual	Todos > 0,80	Nenhum item com inadequação segundo MSA
Matriz de correlações	Policórica; Sweet Smoothing	Perda de 3,6% da covariância
Análise paralela - dimensão 1	53,16% real; 7,48% aleatório (P95)	Retida
Análise paralela - dimensão 2	7,41% real; 6,72% aleatório (P95)	Retida
Análise paralela - dimensão 3	4,67% real; 6,26% aleatório (P95)	Não retida
Número de fatores	2	Indicado pela análise paralela

Fonte: elaboração própria com dados da pesquisa (2026), a partir dos resultados gerados no software FACTOR.

A análise paralela reteve dois fatores, mas o segundo superou por margem limitada o percentil 95 das matrizes aleatórias; essa informação integra a interpretação cautelosa da solução.

A Tabela C4 apresenta as cargas e comunalidades item a item.

Tabela C4. Cargas fatoriais da solução de dois fatores

Item	Fator 1	Fator 2	h ²
GI1	0,442	—	0,395
GI2	0,595	—	0,537
GI3	0,722	—	0,594
GI4	0,470	—	0,388
GI5	0,470	0,318	0,564
EP1	0,868	—	0,685
EP2	0,919	—	0,763
EP3	1,019	—	0,720
EP4	1,144	-0,358	0,776
EP5	0,945	—	0,692
SC1	0,671	—	0,545
SC2	0,398	—	0,400
SC3	0,440	0,316	0,517
SC4	0,452	0,365	0,603
SC5	0,304	0,549	0,663
RC1	0,801	—	0,675

Item	Fator 1	Fator 2	h ²
RC2	0,762	—	0,511
RC3	0,870	—	0,678
RC4	0,941	—	0,639
RC5	0,788	—	0,571
RC6	0,349	0,481	0,623
CE1	—	0,844	0,469
CE2	—	0,554	0,627
CE3	—	0,843	0,599
CE4	—	0,693	0,560
CE5	—	0,652	0,216
CS1	—	0,876	0,563
CS2	—	0,984	0,609
CS3	-0,431	1,120	0,661
CS4	-0,314	0,819	0,355
MP1	0,525	0,354	0,701
MP2	0,480	0,378	0,667
MP3	—	0,420	0,449

Fonte: elaboração própria com dados da pesquisa (2026), a partir dos resultados gerados no software FACTOR. Nota: cargas absolutas inferiores a 0,30 foram omitidas. A matriz padrão deve ser interpretada em conjunto com a correlação entre fatores e com a saída completa do programa.

Os itens de EP e RC concentraram-se no primeiro fator; CE e CS, no segundo. SC5, RC6 e MP apresentaram transversalidade, e três coeficientes da matriz padrão superaram 1, ocorrência que requer interpretação cautelosa conforme discutido na Seção 4.3.

A Tabela C5 compara as três soluções estimadas.

Tabela C5. Comparação das soluções fatoriais

Solução	Análise paralela	RMSEA	CFI/TLI	RMSR	BIC	Síntese
1 fator	Não	0,055	0,989 / 0,989	0,0841	1.197,501	Fator geral; resíduos superiores à solução de 2 fatores
2 fatores	Sim	0,038	0,995 / 0,994	0,0594	1.159,289	Solução retida
7 fatores	Não	0,009	0,999 / 1,000	0,0272	1.761,124	Melhor ajuste absoluto; não retida pela análise paralela; BIC mais alto

Fonte: elaboração própria com dados da pesquisa (2026), a partir dos resultados gerados no software FACTOR.

A solução de dois fatores combinou retenção pela análise paralela, menor BIC e resíduos inferiores aos da solução unidimensional; a solução de sete fatores melhorou o ajuste absoluto, mas não foi retida pela análise paralela e apresentou BIC mais alto.

A Tabela C6 detalha as associações exploratórias utilizadas nas hipóteses.

Tabela C6. Associações exploratórias entre os domínios

Relação	Spearman ρ	p-valor	Interpretação
CE ↔ MGR	0,578	< 0,001	Positiva; compatível com H1
MGR ↔ CS	0,368	< 0,001	Positiva; compatível com H2
CE ↔ CS	0,520	< 0,001	Positiva; compatível com H3
MP ↔ GI	0,515	< 0,001	Positiva
MP ↔ EP	0,652	< 0,001	Positiva
MP ↔ SC	0,597	< 0,001	Positiva
MP ↔ RC	0,678	< 0,001	Positiva
MP ↔ CE	0,601	< 0,001	Positiva
MP ↔ CS	0,385	< 0,001	Positiva
MP ↔ MGR	0,685	< 0,001	Positiva; compatível com H4

Fonte: elaboração própria com dados da pesquisa (2026).

As associações foram positivas e significativas, mas compartilham fonte, respondente e momento de coleta, condição sujeita a efeitos de método comum (Podsakoff *et al.*, 2003), e não autorizam inferência causal.

APÊNDICE D — DETALHAMENTO DA PROPOSTA DE USO SUPERVISÓRIO

Este apêndice sistematiza os domínios, as etapas, as respostas supervisoras e os produtos previstos na proposta. Todo o conteúdo é prospectivo e requer validação antes de uso decisório.

A Tabela D1 consolida os domínios e suas finalidades analíticas.

Tabela D1. Síntese dos domínios do instrumento

Domínio	Itens	Finalidade analítica
GI	5	Governança e integração da gestão de riscos de segurança da informação.
EP	5	Formalização e disciplina dos processos de gestão de riscos.
SC	5	Adequação das práticas ao porte, complexidade e contexto regulatório da EFPC.
RC	6	Risco cibernético, continuidade, incidentes, fornecedores e proteção de dados.
CE	5	Cultura, liderança, conscientização e engajamento em segurança.
CS	4	Comportamento seguro declarado pelo respondente.
MP	3	Maturidade percebida em segurança da informação.

Fonte: elaboração própria. Bases de elaboração declaradas: Oliveira e Nunes (2025), ISO 31000:2018 (ISO, 2018), Ferreira *et al.* (2025) e adaptação autoral ao contexto das EFPC. NIST (2024) e Delso-Vicente *et al.* (2025) foram incorporados posteriormente como sustentação teórica e interpretativa, não como origem dos itens.

Os códigos e denominações devem ser usados de forma uniforme em todo o artigo; a origem item a item permanece dependente do histórico de elaboração.

A Tabela D2 descreve as seis etapas, em correspondência com o fluxo resumido na Seção 5.1.

Tabela D2. Etapas propostas para uso supervisório

Etapas	Descrição	Produto esperado
1. Coleta estruturada	Aplicação do instrumento a profissionais ou unidades com conhecimento sobre governança, riscos, segurança, tecnologia, controles ou gestão institucional.	Base de respostas padronizada.
2. Validação da base	Exclusão de respostas incompletas, inconsistentes ou reprovadas no controle de atenção; tratamento dos itens reversos.	Base válida para análise.
3. Cálculo dos escores	Cálculo dos escores médios por domínio e da Maturidade em Gestão de Riscos de Segurança da Informação.	Escores GI, EP, SC, RC, CE, CS, MP e MGR.
4. Interpretação dos escores	Interpretação dos escores contínuos por domínio e da MGR, com eventual adoção futura de categorias administrativas somente após validação.	Perfil de escores para apoio à interpretação.
5. Cruzamento com criticidade	Combinação da maturidade com critérios institucionais de porte, complexidade, segmento, exposição ou histórico de risco.	Matriz de risco e maturidade.
6. Resposta fiscalizatória	Definição de medida proporcional, como monitoramento, orientação, diligência, supervisão temática ou fiscalização direta.	Possível plano de ação supervisória.

Fonte: elaboração própria com base em IOPS (2023).

A integração conceitual entre maturidade e criticidade é apresentada na Tabela 6 da Seção 5.2. Este apêndice detalha possíveis respostas supervisoras e produtos decorrentes de eventual aplicação futura da proposta.

A Tabela D3 relaciona fragilidades hipotéticas a respostas supervisoras possíveis.

Tabela D3. Situações hipotéticas e respostas possíveis

Situação hipotética	Resposta supervisória possível
Menor MGR associada a alta criticidade	Fiscalização direta ou supervisão específica.
Escore relativamente baixo em RC	Supervisão temática sobre risco cibernético, continuidade, incidentes, fornecedores e proteção de dados.
Escore relativamente baixo em GI	Solicitação de evidências de governança, política, comitês, responsabilidades e decisões.
Escore relativamente baixo em EP	Diligência sobre processo de gestão de riscos, registros, revisões e tratamento de riscos residuais.
Escore relativamente baixo em SC	Avaliação da adequação dos controles ao porte, contexto, terceirização e criticidade da entidade.
Escore relativamente baixo em CE	Ação orientativa sobre cultura, conscientização, liderança e responsabilização.
Escore relativamente baixo em CS	Reforço de capacitação, comunicação, procedimentos e canais de reporte.
Escore relativamente baixo em MP com escores relativamente altos nos domínios	Avaliação da percepção interna, comunicação institucional e clareza das práticas de segurança.
Escores relativamente elevados associados a alta criticidade	Monitoramento periódico com validação amostral de evidências.

Fonte: elaboração própria com base em IOPS (2023).

As respostas não são automáticas nem exaustivas e devem ser calibradas segundo criticidade, evidências e proporcionalidade.

A Tabela D4 apresenta produtos que poderiam ser gerados após validação e implantação gradual.

Tabela D4. Produtos potenciais da proposta

Produto	Finalidade
Escore por dimensão	Identificar forças e fragilidades específicas em eventual aplicação institucional.
Escore consolidado de MGR	Sintetizar percepções sobre gestão de riscos de segurança da informação.
Matriz maturidade-criticidade	Combinar, prospectivamente, escores do instrumento com criticidade institucional externa.
Painel setorial agregado	Acompanhar tendências agregadas em reaplicações futuras.
Relatório de supervisão temática	Apoiar, futuramente, ações sobre dimensões selecionadas.
Plano de acompanhamento	Registrar, em eventual aplicação supervisória, recomendações, prazos, responsáveis e evolução.
Série histórica	Examinar, após reaplicações, estabilidade ou mudança dos escores ao longo do tempo.

Fonte: elaboração própria com base em IOPS (2023).

Painel setorial, série histórica e plano de acompanhamento são produtos potenciais; não foram produzidos ou avaliados nesta pesquisa.

APÊNDICE E — INSTRUMENTO APLICADO

Este apêndice reproduz integralmente o conteúdo da versão final apresentada aos participantes: apresentação da pesquisa, declaração de participação, seis itens de perfil, escala de resposta, 33 itens psicométricos e um item de controle de atenção. A organização editorial abaixo omite apenas elementos visuais da plataforma, sem alterar os enunciados, as alternativas ou a ordem dos blocos.

E.1. Apresentação da pesquisa e participação voluntária

Pesquisa acadêmica EFPC - Segurança da Informação e Risco Cibernético

Esta pesquisa integra artigo científico da Especialização em Privacidade e Segurança da Informação da Universidade de Brasília - UnB.

O objetivo é coletar percepções de profissionais que atuam ou possuem experiência com Entidades Fechadas de Previdência Complementar - EFPC sobre governança, gestão de riscos de segurança da informação, risco cibernético, continuidade e cultura de segurança.

A pesquisa é anônima. Não serão solicitados nome da EFPC, CNPJ, nome do respondente, e-mail, cidade ou qualquer dado que permita identificação direta da entidade ou da pessoa respondente.

As respostas serão analisadas de forma agregada, com finalidade exclusivamente acadêmica e científica.

Tempo estimado de resposta: 8 a 12 minutos.

Participação voluntária e anonimato

Antes de responder, confirme que compreendeu a finalidade acadêmica da pesquisa, o caráter anônimo das respostas e a análise agregada dos dados.

Declaração de participação

Li as informações iniciais e concordo em participar voluntariamente da pesquisa.

Nota editorial: o asterisco exibido na plataforma indicava resposta obrigatória. Todas as perguntas reproduzidas neste apêndice eram obrigatórias.

E.2. Bloco A — Perfil do Respondente

Objetivo: caracterizar o perfil geral dos respondentes, sem identificar a EFPC ou a pessoa respondente.

Código	Pergunta	Alternativas
PR1	Principal área de atuação relacionada à sua experiência com EFPC	Alta administração/Diretoria; Conselho deliberativo, conselho fiscal ou comitê estatutário; Riscos, controles internos, compliance ou governança; Auditoria; Tecnologia da Informação ou Segurança da Informação; Jurídico, privacidade ou proteção de dados; Área operacional, benefícios, atendimento ou investimentos; Outra.
PR2	Tempo de experiência no setor de previdência complementar	Até 2 anos; De 3 a 5 anos; De 6 a 10 anos; Mais de 10 anos.
PR3	Porte percebido da EFPC	Pequeno porte; Médio porte; Grande porte.
PR4	Grau percebido de terceirização de serviços de TI/segurança da informação	Baixo; Médio; Alto.
PR5	A EFPC possui Política de Segurança da Informação formalmente aprovada?	Sim; Não.
PR6	A EFPC passou por auditoria, avaliação externa ou diagnóstico estruturado de segurança da informação/cibersegurança nos últimos 2 anos?	Sim; Não.

E.3. Escala de resposta

Para os blocos de afirmações, utilize a seguinte escala:

Valor	Resposta
1	Discordo totalmente
2	Discordo parcialmente
3	Nem concordo nem discordo
4	Concordo parcialmente
5	Concordo totalmente

E.4. Itens psicométricos

Bloco B — Governança e Integração — GI

Definição operacional: grau em que a gestão de riscos de segurança da informação está integrada à governança, ao planejamento e à tomada de decisão da EFPC.

Código	Afirmação
GI1	A alta administração e/ou os órgãos de governança consideram riscos de segurança da informação em decisões estratégicas da EFPC.

Código	Afirmação
GI2	A gestão de riscos de segurança da informação está integrada ao planejamento estratégico da EFPC.
GI3	Existe uma política formal que orienta a gestão de riscos de segurança da informação na EFPC.
GI4	Diferentes áreas da EFPC, e não apenas a área de TI, participam das discussões sobre riscos de segurança da informação.
GI5	A gestão de riscos de segurança da informação é considerada em processos críticos da EFPC, como benefícios, investimentos, cadastro, atendimento ou relacionamento com participantes.

Bloco C — Estrutura e Disciplina de Processo — EP

Definição operacional: grau de formalização, padronização e consistência dos processos de gestão de riscos de segurança da informação.

Código	Afirmação
EP1	Existe processo formal documentado para identificação, análise, tratamento e acompanhamento de riscos de segurança da informação.
EP2	A EFPC utiliza metodologia padronizada para gestão de riscos de segurança da informação.
EP3	Os riscos de segurança da informação são registrados em repositório estruturado e atualizado periodicamente.
EP4	A EFPC realiza revisões periódicas dos riscos de segurança da informação identificados.
EP5	A EFPC utiliza indicadores, métricas ou evidências para acompanhar a efetividade dos controles de segurança da informação.

Bloco D — Sensibilidade ao Contexto — SC

Definição operacional: capacidade da EFPC de adaptar suas práticas de segurança da informação e gestão de riscos às suas características institucionais, regulatórias e operacionais.

Código	Afirmação
SC1	A gestão de riscos de segurança da informação é adaptada ao porte, à complexidade e ao modelo operacional da EFPC.
SC2	As decisões sobre riscos de segurança da informação consideram o contexto regulatório aplicável às EFPC.
SC3	Os controles de segurança da informação são definidos com base nas necessidades específicas da EFPC, e não apenas para cumprir exigências mínimas.
SC4	As práticas de segurança da informação são ajustadas quando ocorrem mudanças relevantes no ambiente tecnológico, regulatório ou operacional.
SC5	As prioridades de segurança da informação refletem a criticidade dos ativos, dados e serviços essenciais aos participantes e assistidos.

Bloco E — Risco Cibernético e Continuidade — RC

Definição operacional: grau em que a EFPC identifica, avalia, trata e monitora riscos cibernéticos, incluindo continuidade dos serviços digitais, incidentes, fornecedores e proteção de dados.

Código	Afirmação
--------	-----------

Código	Afirmação
RC1	A EFPC possui práticas definidas para identificar e tratar ameaças cibernéticas relevantes ao seu contexto de atuação.
RC2	A EFPC possui Plano de Continuidade de Negócios, Plano de Recuperação de Desastres ou procedimento equivalente que contemple riscos cibernéticos.
RC3	A EFPC monitora indicadores de risco cibernético, como tentativas de acesso indevido, phishing, incidentes, vulnerabilidades ou indisponibilidades relevantes.
RC4	A EFPC possui procedimentos formais para resposta, tratamento e comunicação de incidentes de segurança da informação.
RC5	A EFPC avalia periodicamente riscos de segurança da informação associados a fornecedores, prestadores de serviços ou terceiros relevantes.
RC6	A proteção dos dados pessoais de participantes, assistidos e beneficiários é tratada como prioridade na gestão de riscos de segurança da informação.

Item de Controle de Atenção

Este item será utilizado apenas para controle de qualidade da base.

Código	Afirmação
AC1	Para fins de controle de qualidade da pesquisa, selecione a opção “Concordo parcialmente” nesta afirmação.

Bloco F — Cultura e Engajamento em Segurança — CE

Definição operacional: grau em que valores, comportamentos, lideranças e práticas internas favorecem uma cultura efetiva de segurança da informação.

Código	Afirmação
CE1	As pessoas que atuam na EFPC compreendem seu papel na proteção das informações e na gestão de riscos de segurança da informação.
CE2	A EFPC promove ações regulares de conscientização em segurança da informação, como treinamentos, campanhas, comunicados ou orientações internas.
CE3	Na EFPC, adotar comportamentos seguros no uso de sistemas, dados e informações é uma expectativa clara para todos.
CE4	As lideranças da EFPC incentivam ativamente boas práticas de segurança da informação e gestão de riscos.
CE5	Na EFPC, as práticas de segurança da informação são vistas principalmente como obrigação burocrática, e não como parte relevante do trabalho.

Bloco G — Comportamento Seguro Declarado — CS

Definição operacional: percepção do respondente sobre a adoção habitual de práticas seguras no exercício de suas atividades.

Código	Afirmação
CS1	Sigo as políticas e orientações de segurança da informação aplicáveis ao meu trabalho.
CS2	Tenho cuidado ao lidar com mensagens, links, anexos e solicitações recebidas por e-mail ou outros canais digitais.
CS3	Comunico ao setor responsável quando identifico incidente, suspeita de incidente ou situação de risco envolvendo segurança da informação.
CS4	Quando estou com pressa, acabo deixando de lado alguns cuidados de segurança da informação.

Bloco H — Maturidade Percebida em Segurança da Informação — MP

Definição operacional: percepção geral do respondente sobre o nível de estruturação da segurança da informação na EFPC.

Código	Afirmação
MP1	De forma geral, considero que a EFPC possui práticas estruturadas de segurança da informação.
MP2	De forma geral, considero que a EFPC está preparada para lidar com riscos cibernéticos relevantes.
MP3	De forma geral, considero que a EFPC evoluiu nos últimos anos em relação à segurança da informação e à gestão de riscos cibernéticos.

E.5. Notas de codificação

CE5 e CS4 foram tratados como itens inversos e recodificados pela expressão 6 - resposta, conforme descrito na Seção 3.3. No AC1, a resposta esperada era 4 - Concordo parcialmente. Essas informações são apresentadas para transparência analítica; no formulário, o AC1 já continha a instrução correspondente.

Fonte: formulário eletrônico final fornecido pelo autor e aplicado entre 22 de junho e 31 de julho de 2026.