



**Governo do Estado de São Paulo
Fundação de Previdência Complementar do Estado de São Paulo
Contratos e Licitações**

TERMO DE REFERÊNCIA

Nº do Processo: 271.00000513/2026-96

Interessado: Fundação de Previdência Complementar do Estado de São Paulo

Assunto: Contratação Seguro Cyber

TERMO DE REFERÊNCIA PREVCOM Nº 034/2026

Processo Administrativo SEI nº 271.00000513/2026-96

1. CONDIÇÕES GERAIS DA CONTRATAÇÃO

1.1. A presente contratação tem por objeto a contratação de apólice de seguro de riscos cibernéticos (“Seguro Cyber”), com cobertura ampla e especializada, voltada à proteção da Fundação de Previdência Complementar do Estado de São Paulo – PREVCOM contra impactos decorrentes de incidentes cibernéticos, conforme condições e exigências estabelecidas neste Termo de Referência.

1.2. Em caso de divergência entre a descrição do item do catálogo do sistema Compras.gov.br e as disposições deste Termo de Referência, prevalecem as disposições deste Termo de Referência.

1.3. Este Termo de Referência foi elaborado em conformidade com o Regulamento de Contratações e Gestão de Bens e Serviços da Fundação de Previdência Complementar do Estado de São Paulo.

1.4. O objeto desta contratação não se enquadra como serviço de luxo, observando o disposto no Decreto estadual nº 67.985, de 27 de setembro de 2023.

1.5. O serviço é caracterizado como serviço contínuo, sem regime de dedicação exclusiva de mão de obra e sem predominância de mão de obra.

1.6. Vigência

O prazo de vigência da contratação é de 12 (doze) meses, contados da emissão da apólice, nos termos do art. 106 da Lei nº 14.133/2021.

1.7. Subcontratação

É vedada a subcontratação dos serviços essenciais da apólice, especialmente aqueles relacionados à emissão, gestão, regulação e liquidação de sinistros. A subcontratação de serviços acessórios somente será admitida mediante autorização expressa da Contratante, desde que não comprometa a qualidade, a confidencialidade, a segurança da informação ou a responsabilidade integral da Contratada.

2. FUNDAMENTAÇÃO E DESCRIÇÃO DA NECESSIDADE

2.1. A fundamentação da contratação encontra-se pormenorizada no Estudo Técnico Preliminar nº 034/2026, apêndice deste Termo de Referência.

2.2. O objeto está previsto no Plano de Contratações Anual 2026 da PREVCOM, conforme apresentado no documento de formalização de demanda DTI nº 0084480595 do processo SEI 271.00000716/2025-00.

2.3. A contratação será realizada nos termos da Lei Federal nº 14.133/2021, observando os princípios da economicidade, eficiência, sustentabilidade, vantajosidade e interesse público. A especificação técnica está alinhada à necessidade institucional de mitigação dos impactos financeiros, operacionais, jurídicos e reputacionais decorrentes de incidentes cibernéticos, aos quais a PREVCOM está permanentemente exposta em razão da natureza de suas atividades e do volume de dados pessoais e financeiros que custodia.

3. DESCRIÇÃO DA SOLUÇÃO – CICLO DE VIDA DO OBJETO

3.1. A solução consiste na contratação de apólice de seguro de riscos cibernéticos (“Seguro Cyber”), com cobertura ampla e especializada, voltada à proteção da PREVCOM contra incidentes cibernéticos que possam comprometer seus ativos digitais, a continuidade de seus serviços, a confidencialidade dos dados pessoais e financeiros e sua imagem institucional.

3.1. Ciclo de Vida

3.1.1. Formalização

- Autorização da contratação: expedição do ato autorizativo competente, nos termos da legislação vigente, habilitando o início do processo de contratação do seguro;
- Emissão da Ordem de Fornecimento da Apólice: documento que formaliza a instrução à seguradora para emissão da apólice, estabelecendo os parâmetros contratados, incluindo coberturas, limites máximos de indenização (LMI), franquias e prazo de vigência.

3.1.2. Emissão da Apólice

- Instrumento contratual que consolida as coberturas contratadas, os limites máximos de indenização (LMI), as franquias, os prazos de vigência, as condições de acionamento e os procedimentos de comunicação de sinistro, devendo ser encaminhado ao contratante no prazo estabelecido em contrato após a emissão da Ordem de Fornecimento.

3.1.3. Execução e Acompanhamento

- Compreende as atividades de gestão contratual durante a vigência da apólice, incluindo:
- monitoramento contínuo da vigência e das condições contratuais;
- gestão de sinistros, com acompanhamento de abertura, instrução e liquidação;
- revisão periódica das coberturas, verificando sua adequação ao perfil de risco do contratante;
- interação com a seguradora para esclarecimentos, atualizações e eventuais endossos.

3.1.4. Encerramento e Avaliação

Ao final da vigência contratual, deverão ser realizadas:

- análise dos sinistros ocorridos e dos resultados da cobertura contratada;
- avaliação da efetividade das coberturas frente aos incidentes registrados no período;
- elaboração de relatório conclusivo subsidiando eventual renovação ou revisão do objeto para novo processo de contratação.

3.2. Coberturas Mínimas Exigidas

3.2.1. Responsabilidade Civil perante Terceiros

- a) Violação de privacidade e confidencialidade: cobertura para responsabilidade civil decorrente de vazamento, perda ou exposição não autorizada de dados pessoais, sensíveis ou confidenciais de terceiros, incluindo obrigações previstas na LGPD;
- b) Segurança de rede: cobertura para danos causados a terceiros em razão de falhas na segurança da infraestrutura tecnológica da PREVCOM, incluindo incidentes originados em fornecedores ou prestadores com acesso aos seus sistemas e dados;
- c) Responsabilidade de mídia: cobertura para reclamações decorrentes de conteúdo digital publicado pela PREVCOM, incluindo violação de direitos autorais, difamação e uso indevido de dados em meios eletrônicos;
- d) Custos regulatórios e multas: cobertura de multas e penalidades administrativas impostas por órgãos reguladores, inclusive a ANPD, em decorrência de falhas de segurança e descumprimento da LGPD, quando seguráveis nos termos da legislação vigente.

3.2.2. Gerenciamento de Crise

- a) Custos de resposta a violação de dados: cobertura das despesas incorridas para contenção, análise e remediação de incidentes cibernéticos, incluindo investigação forense e recuperação de sistemas afetados;
- b) Custos de identificação e preservação de dados: cobertura para atividades de identificação do escopo do vazamento e preservação de evidências digitais para fins legais e regulatórios;
- c) Custos de consultoria jurídica: cobertura para honorários advocatícios relativos à gestão do incidente, defesa administrativa perante reguladores e orientação sobre obrigações legais decorrentes do evento;
- d) Custos de consultoria sobre indenização a terceiros: cobertura para assessoria especializada na avaliação e negociação de indenizações devidas aos titulares de dados ou terceiros afetados;
- e) Custos de *call center* e notificação: cobertura das despesas com estruturação e operação de canal de atendimento aos titulares de dados afetados; notificação obrigatória aos titulares nos termos da LGPD; comunicação à ANPD nos prazos legais; e custos de monitoramento de crédito para os titulares impactados;
- f) Custos de consultoria de imagem: cobertura para serviços de relações públicas e gerenciamento reputacional voltados à contenção de danos à imagem institucional da PREVCOM decorrentes do incidente.

3.2.3. Perdas Diretas do Segurado

- a) Extorsão cibernética: cobertura para eventos de *ransomware* e demais modalidades de extorsão cibernética, incluindo custos de negociação, pagamento quando autorizado e recuperação dos sistemas e dados afetados;
- b) Interrupção de negócios: cobertura de perdas operacionais e financeiras decorrentes de paralisação ou indisponibilidade dos serviços da PREVCOM causadas por incidente cibernético coberto;
- c) Fraude eletrônica: cobertura para perdas financeiras originárias de engenharia social, incluindo desvios decorrentes de comprometimento de e-mail corporativo (BEC – *Business Email Compromise*).

3.2.4. Disposições Gerais sobre as Coberturas

Independentemente do módulo de cobertura, a apólice deverá observar as seguintes condições mínimas:

- a) Cobertura retroativa: data retroativa a ser negociada e definida na apólice, de modo a abranger incidentes cujos efeitos se manifestem durante a vigência, mas cuja origem seja anterior à contratação;
- b) Período estendido de descoberta de sinistros (*extended reporting period*): prazo mínimo de 12 (doze) meses após o término da vigência da apólice para comunicação de sinistros cujos fatos geradores tenham ocorrido durante a cobertura;
- c) Cobertura para incidentes de cadeia de fornecimento: a cobertura se estende a incidentes originados em fornecedores, prestadores de serviços ou quaisquer terceiros com acesso aos sistemas, redes ou dados da PREVCOM, tanto para fins de responsabilidade civil perante terceiros quanto para cobertura de perdas diretas do segurado.

4. REQUISITOS DA CONTRATAÇÃO

4.1. A contratação deve selecionar seguradora devidamente autorizada pela Superintendência de Seguros Privados (SUSEP) para emissão e gestão de apólice de Seguro Cyber.

4.2. Limite Mínimo de Cobertura

O limite mínimo da apólice deverá ser de R\$ 10.000.000,00 (dez milhões de reais), valor fundamentado no perfil de risco da PREVCOM enquanto entidade de previdência complementar custodiante de dados financeiros e previdenciários classificados como sensíveis nos termos do art. 5º, II, da Lei nº 13.709/2018 (LGPD).

4.2.1. A memória de cálculo utilizada para definição do limite estimado da contratação encontra-se detalhada no Estudo Técnico Preliminar – ETP nº 034/2026.

4.2.2. Sublimites mínimos por módulo de cobertura

A proposta deverá discriminar expressamente os sublimites aplicáveis a cada módulo, observados os valores mínimos abaixo:

Módulo	Sublimite mínimo
Responsabilidade civil perante terceiros	R\$ 10.000.000,00
Gerenciamento de crise (agregado)	R\$ 4.000.000,00
— Resposta a incidente e investigação forense	R\$ 1.000.000,00
— Notificação, call center e monitoramento de crédito	R\$ 1.000.000,00
— Consultoria jurídica	R\$ 500.000,00
— Consultoria de imagem e relações públicas	R\$ 500.000,00
— Identificação e preservação de dados	R\$ 500.000,00
Perdas diretas do segurado (agregado)	R\$ 3.000.000,00
— Interrupção de negócios	R\$ 3.000.000,00
— Extorsão cibernética	R\$ 1.000.000,00
— Fraude eletrônica e BEC	R\$ 500.000,00
Custos regulatórios e multas	R\$ 2.500.000,00
Limite agregado total	R\$ 10.000.000,00

4.2.3. Revisão do limite

O limite mínimo de cobertura deverá ser revisado por ocasião de cada renovação contratual, considerando:

variação do volume de titulares de dados sob custódia da PREVCOM;

atualização do índice de custo médio por registro comprometido divulgado por relatórios de referência do setor (*IBM Cost of a Data Breach* ou equivalente);

histórico de sinistros registrados durante a vigência anterior;

eventuais alterações na regulamentação da ANPD que impliquem elevação do teto de penalidades aplicáveis.

4.3. Franquias, carências e exclusões

A proposta deverá discriminar expressamente as franquias aplicáveis por cobertura, as principais exclusões e eventuais carências, sendo vedada a aceitação de apólice com franquias desproporcionais ao porte do risco ou com exclusões que comprometam as coberturas mínimas exigidas neste TR.

4.4. Vigência da apólice

O prazo de vigência da apólice será de 36 (trinta e seis) meses, com início imediatamente após emissão da Ordem de Fornecimento.

4.5. Qualificação técnica da seguradora

A Contratada deverá:

4.5.1. Possuir registro ativo e regular perante a SUSEP;

4.5.2. Dispor de equipe especializada em gestão de crise cibernética;

4.5.3. Possuir infraestrutura para atendimento nacional, com canal exclusivo para acionamento da apólice, disponível 24 horas por dia, 7 dias por semana.

4.6. Segurança da informação e privacidade

4.6.1. Observar integralmente a LGPD e demais normas aplicáveis à proteção de dados pessoais;

4.6.2. Garantir a confidencialidade das informações tratadas durante a vigência da apólice;

4.6.3. Adotar protocolos seguros para comunicação e gestão de sinistros;

4.6.4. Observar, quando aplicável, a integração com os planos de continuidade de negócios e de resposta a incidentes da PREVCOM.

4.7. Garantia, manutenção e assistência técnica

4.7.1. Garantir a cobertura integral da apólice durante toda a vigência contratual.

4.7.2. Disponibilizar atendimento técnico especializado, observando os seguintes SLAs por severidade do incidente:

Severidade	Tipo de Incidente	Prazo de Atendimento
Crítica	Ransomware, exfiltração em andamento	Até 4 horas
Alta	Incidente de alta severidade confirmado	Até 8 horas
Demais	Regulação e liquidação formal	Até 24 horas

4.8. Metodologia de trabalho

4.8.1. Adotar metodologia baseada em gestão de riscos, governança e boas práticas aplicáveis

ao mercado de seguros cibernéticos;

4.8.2. Estabelecer procedimentos claros para acionamento da apólice, atendimento emergencial, regulação e gestão de sinistros;

4.8.3. Manter comunicação tempestiva, formal e adequada com a contratante.

4.9. Vedações e restrições

Fica vedada a contratação de seguradora:

4.9.1. Que não possua registro ativo perante a SUSEP;

4.9.2. Que esteja declarada inidônea ou suspensa de contratar com a Administração Pública;

4.9.3. Que não comprove capacidade técnica para emissão de apólice de seguro cibernético;

4.9.4. Que apresente apólice com exclusões que comprometam as coberturas mínimas exigidas neste TR.

5. MODELO DE EXECUÇÃO DO OBJETO

5.1. A execução terá início após a emissão da Ordem de Fornecimento e a emissão da respectiva apólice pela Contratada.

5.2. A apólice deverá ser emitida conforme os termos do edital, da proposta vencedora, do contrato e deste TR, contemplando coberturas, limites, sublimites, franquias, exclusões, prazos e condições de acionamento.

5.3. A apólice terá vigência de 36 (trinta e seis) meses, contados da data definida no contrato.

5.4. A Contratada deverá disponibilizar canal exclusivo para atendimento emergencial, acionamento da apólice e suporte técnico, jurídico e operacional em caso de incidente cibernético.

5.5. A apólice entrará em vigor imediatamente após a emissão da Ordem de Fornecimento e a comprovação da cobertura.

5.1. Gestão da apólice

5.1.1. A PREVCOM designará gestor e fiscal responsáveis pelo acompanhamento da execução contratual, incluindo monitoramento da vigência, análise de relatórios e interação com a Contratada em situações de crise.

5.1.2. A Contratada deverá disponibilizar plataforma digital para acompanhamento da apólice, dos acionamentos e sinistros.

5.1.3. A Contratada deverá participar de reuniões técnicas de acompanhamento quando convocada pela PREVCOM.

5.2. Acionamento em caso de sinistro

5.2.1. A PREVCOM deverá comunicar imediatamente à Contratada qualquer incidente que possa configurar sinistro.

5.2.2. A Contratada deverá iniciar o atendimento conforme os SLAs estabelecidos no item 4.4.2 deste TR.

5.2.3. A regulação e liquidação do sinistro deverão ocorrer com base na documentação técnica fornecida pela Contratante, respeitados os prazos legais, contratuais e securitários aplicáveis.

6. MODELO DE GESTÃO DA CONTRATAÇÃO

6.1. O contrato deverá ser executado fielmente pelas partes, de acordo com as cláusulas avençadas e as normas da Lei nº 14.133, de 2021, e cada parte responderá pelas

consequências de sua inexecução total ou parcial.

6.2. Em caso de impedimento, ordem de paralisação ou suspensão do contrato, o cronograma de execução será prorrogado automaticamente pelo tempo correspondente, anotadas tais circunstâncias mediante simples apostila.

6.3. As comunicações entre o CONTRATANTE e o CONTRATADO devem ser realizadas por escrito sempre que o ato exigir tal formalidade, admitindo-se o uso de mensagem eletrônica para esse fim.

6.4. O CONTRATANTE poderá convocar representante do CONTRATADO para adoção de providências que devam ser cumpridas de imediato.

6.5. Após a celebração da contratação, o CONTRATANTE poderá convocar o representante do CONTRATADO para reunião inicial para apresentação do plano de fiscalização, que conterá informações acerca das obrigações contratuais, dos mecanismos de fiscalização, das estratégias para execução do objeto, do plano complementar de execução do CONTRATADO, quando houver, do método de aferição dos resultados e das sanções aplicáveis, dentre outros.

6.6. A execução do contrato deverá ser acompanhada pelo gestor do contrato e fiscalizada pelo(s) fiscal(is) do contrato, ou pelo(s) respectivo(s) substituto(s), nos termos dos artigos 106 a 110 do RGC.

Preposto

6.7. O CONTRATADO designará formalmente o seu preposto, antes do início da prestação dos serviços, indicando no instrumento os poderes e deveres em relação à execução do objeto contratado.

6.8. O CONTRATANTE poderá recusar, desde que justificadamente, a indicação ou a manutenção do preposto do CONTRATADO, hipótese em que o CONTRATADO designará outro para o exercício da atividade.

Gestor do Contrato

6.9. O gestor do contrato é o responsável pelo acompanhamento da execução contratual sob o enfoque administrativo, competindo-lhe coordenar a atuação dos fiscais e conduzir as atividades de natureza burocrática da gestão do contrato, incluindo controle de prazos referentes ao contrato, verificação documental, tramitação de ajustes contratuais, registros nos sistemas oficiais e adoção das providências necessárias para assegurar a regularidade da execução.

6.10. Compete ao gestor do contrato:

- a) acompanhar a execução do contrato em todas as suas fases, com o apoio dos fiscais designados;
- b) coordenar a fiscalização, estabelecendo rotinas de monitoramento, comunicação e integração entre os agentes envolvidos;
- c) controlar os prazos e obrigações administrativas do contrato, tais como vigência, garantias, reajustes, prorrogações, encerramento e cronograma de pagamentos;
- d) verificar a conformidade das notas fiscais apresentadas e da documentação exigida para o pagamento, incluindo folha de pagamento, certidões fiscais e trabalhistas, regularidade junto ao CADIN ESTADUAL, ao FGTS e demais obrigações legais;
- e) averiguar, nos contratos com dedicação exclusiva de mão de obra, o cumprimento das obrigações trabalhistas e previdenciárias pela contratada, mediante conferência da folha de pagamento e dos recolhimentos de encargos legais;
- f) manter organizados e arquivados, na Plataforma SEI, todos os documentos relacionados à execução contratual, conforme critérios de transparência, rastreabilidade e gestão documental da Prevcom;

- g) analisar solicitações de reequilíbrio econômico-financeiro, alterações contratuais, reajustes e prorrogações apresentadas pela contratada;
- h) iniciar e conduzir os procedimentos administrativos relacionados a aditivos, revisões contratuais, pagamentos, suspensões e encerramento do contrato;
- i) suspender, de forma justificada, a entrega de bens ou a prestação de serviços, sempre que houver risco à regularidade da execução contratual;
- j) assegurar a inserção e a atualização do contrato e de suas alterações nos sistemas oficiais de transparência e gestão contratual, tais como o PNCP, o Sistema AUDESP/TCE e o sítio eletrônico da Prevcom;
- k) assegurar a publicidade e a transparência dos atos praticados no âmbito da execução contratual, em conformidade com os princípios da administração pública;
- l) emitir o ateste definitivo da execução contratual, nos termos do artigo 112 do RGC, após a verificação das condições técnicas e documentais exigidas para o pagamento;
- m) elaborar o relatório final da execução do contrato, consolidando as informações prestadas pelos fiscais e os registros constantes do processo administrativo; e
- n) adotar as providências necessárias para a instauração de processo administrativo de responsabilização da contratada, quando constatada infração contratual ou descumprimento das obrigações assumidas.

6.11. As atribuições acima previstas deverão ser exercidas com base nos princípios da legalidade, eficiência, controle, razoabilidade, economicidade e gestão de riscos.

6.12. É dever do gestor atuar com diligência, zelo e observância aos princípios da administração pública, adotando todas as medidas necessárias para o cumprimento adequado e eficiente das obrigações contratuais.

6.13. O gestor poderá ser responsabilizado administrativa, civil e penalmente por omissão injustificada, negligência ou descumprimento dos deveres estabelecidos neste Regulamento e demais normas aplicáveis.

Fiscal(is)

6.14. O fiscal do contrato é o agente responsável pelo acompanhamento da execução contratual sob o enfoque técnico e operacional, competindo-lhe verificar a conformidade dos bens ou serviços com as especificações contratuais, realizar medições, registrar ocorrências e subsidiar tecnicamente o gestor para a tomada de decisões e para a regularidade da execução.

6.15. Compete ao fiscal técnico do contrato:

- a) acompanhar a execução do objeto contratado, presencialmente ou por meio documental, verificando sua aderência às condições técnicas estabelecidas no contrato e nos eventuais aditivos;
- b) realizar medições de serviços e verificar a conformidade das entregas de bens com os quantitativos, prazos e padrões de qualidade definidos contratualmente;
- c) conferir e atestar planilhas, relatórios, faturas e demais documentos que comprovem a execução do objeto, incluindo o preenchimento do ateste provisório, conforme o artigo 112 do RGC;
- d) registrar, em relatório ou documento específico, todas as ocorrências técnicas relevantes, com sugestões de medidas corretivas, comunicando-as tempestivamente ao gestor;
- e) propor ao gestor, quando cabível, a suspensão da execução, a prorrogação de prazos, a aplicação de penalidades ou a necessidade de ajustes contratuais, com base na verificação técnica da execução;
- f) apoiar o gestor na elaboração do ateste definitivo e na avaliação do desempenho da

contratada, fornecendo os subsídios técnicos necessários;

g) zelar pelo cumprimento das normas técnicas, legais e contratuais, adotando medidas preventivas de controle da execução e assegurando a rastreabilidade dos atos de fiscalização;

h) o fiscal deverá atuar com diligência, observando os princípios da legalidade, eficiência, transparência e economicidade, respondendo administrativa, civil e penalmente pelo desempenho de suas funções.

6.16. É vedado ao fiscal negociar cláusulas contratuais ou valores diretamente com a contratada, salvo mediante ciência e autorização expressa do gestor do contrato, devidamente formalizadas por meio de aditivo contratual ou ato jurídico equivalente.

6.17. O fiscal deverá assegurar que o acompanhamento da execução seja preventivo, contínuo e sistemático, com documentação adequada e tempestiva das ações de fiscalização.

7. INSTRUMENTOS DE AVALIAÇÃO E ACOMPANHAMENTO

7.1. Indicadores de desempenho

- a) Tempo de resposta após acionamento da apólice, conforme SLAs por faixa de severidade;
- b) Tempo de regulação e liquidação de sinistros;
- c) Efetividade das ações de suporte técnico, jurídico e de comunicação;
- d) Grau de satisfação da PREVCOM com o atendimento prestado;
- e) Conformidade com prazos e cláusulas contratuais.

7.2. Gestão de riscos e contingência

A PREVCOM manterá plano de contingência para situações de falha na cobertura ou atraso na resposta da seguradora. A seguradora deverá apresentar plano de continuidade de atendimento em caso de indisponibilidade operacional.

7.3. Comunicação e transparência

Toda comunicação entre contratante e contratada será registrada formalmente no sistema eletrônico oficial. Reuniões de acompanhamento serão realizadas trimestralmente, podendo ser convocadas extraordinariamente em caso de sinistro ou incidente relevante.

7.4. Auditoria e controle

O contrato estará sujeito à auditoria interna e externa, conforme diretrizes da PREVCOM e dos órgãos de controle competentes. A seguradora deverá colaborar com o fornecimento de informações e documentos sempre que solicitado.

8. FORMA E CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

8.1. Critério de julgamento

A seleção da proposta vencedora dar-se-á pelo critério de **menor valor do prêmio**, nos termos do art. 33, I, da Lei nº 14.133/2021, desde que a proposta atenda integralmente aos requisitos técnicos mínimos estabelecidos neste Termo de Referência, especialmente quanto às coberturas previstas no item 3.

8.2. Habilitação jurídica

Inscrição do ato constitutivo no registro competente, conforme a natureza jurídica do licitante, acompanhada de documento comprobatório de seus administradores.

- a) Cadastro Nacional da Pessoa Jurídica – CNPJ;

- b) Ato constitutivo, estatuto ou contrato social em vigor, devidamente registrado no órgão competente;
- c) No caso de sociedades por ações, ata arquivada da assembleia de eleição da última diretoria;
- d) Inscrição do ato constitutivo nos órgãos próprios de registro e controle de profissionais ou sociedades, quando exigido por regulamentação específica; e
- e) Decreto de autorização arquivado, no caso de empresa ou sociedade estrangeira em funcionamento no País.

8.3. Habilitação fiscal, social, trabalhista e idoneidade

- a) Certidão de regularidade perante o Cadastro Informativo de Créditos Não Quitados do Setor Público – Cadin estadual de São Paulo;
- b) Certidão de regularidade com créditos tributários federais e da Dívida Ativa da União (INSS);
- c) Certificado de regularidade do Fundo de Garantia do Tempo de Serviço – FGTS;
- d) Certidão negativa de débitos trabalhistas (CNDT); e
- e) Declaração de que não emprega menores de dezoito em trabalho noturno, perigoso ou insalubre, e de qualquer trabalho a menores de dezesseis anos, salvo na condição de aprendiz, a partir de quatorze anos, em cumprimento do disposto no inciso XXXIII do art. 7º da Constituição Federal;
- f) Certidão de Apenados de Impedimentos de Contrato e Licitação emitida pelo Tribunal de Contas do Estado de São Paulo; e
- g) Certidão Negativa Correccional, emitida pela Controladoria Geral da União.

8.4. Qualificação econômico-financeira

- Certidão negativa de falência;
- Balanço patrimonial e demonstrações contábeis dos 2 (dois) últimos exercícios, com índices de Liquidez Geral (LG), Liquidez Corrente (LC) e Solvência Geral (SG) superiores a 1.

8.5. Qualificação técnica

- Autorização vigente da SUSEP para operação no ramo de seguro cibernético;
- Comprovação de estrutura de atendimento emergencial disponível 24h/7d.

9. INFRAÇÕES, SANÇÕES E GLOSAS

O descumprimento total ou parcial das cláusulas contratuais, das especificações técnicas ou das obrigações legais poderá ensejar a aplicação das sanções previstas na Lei nº 14.133/2021.

9.1. Infrações passíveis de sanção

- a) Não emitir ou atrasar injustificadamente a emissão da apólice;
- b) Recusar ou atrasar injustificadamente a regulação de sinistros devidamente comunicados;
- c) Descumprir os SLAs de atendimento emergencial previstos neste TR;
- d) Omitir ou prestar informações falsas em relatórios ou comunicações oficiais;
- e) Violar a confidencialidade dos dados, especialmente os protegidos pela LGPD;

f) Executar parcialmente ou deixar de executar o contrato sem justificativa aceita pela Administração;

g) Realizar subcontratação irregular ou sem autorização expressa da PREVCOM.

9.2. Sanções aplicáveis

As sanções observarão o disposto nos arts. 156 a 162 da Lei nº 14.133/2021, aplicadas de forma graduada conforme a natureza, a gravidade e a reincidência da infração, nos termos a seguir:

9.2.1. Advertência

Aplicável nos casos de descumprimento de obrigações acessórias de baixo impacto, desde que não haja reincidência e o fato não cause prejuízo à continuidade da cobertura ou ao acionamento da apólice, incluindo:

a) atraso na entrega de documentos ou relatórios exigidos no TR por prazo de até 5 (cinco) dias úteis;

b) falhas formais na comunicação com o gestor do contrato, sem prejuízo ao segurado.

9.2.2. Multa moratória

Aplicável pelo atraso injustificado no cumprimento de obrigações contratuais com prazo definido, à razão de 0,5% (meio por cento) por dia de atraso, calculada sobre o valor do prêmio anual da apólice, limitada a 10% (dez por cento) do mesmo valor, nas seguintes hipóteses:

1. atraso na emissão da apólice após a Ordem de Fornecimento;
2. atraso no envio de endosso solicitado pela PREVCOM;
3. atraso na confirmação de recebimento de comunicação de sinistro;
4. atraso no início do atendimento após acionamento formal da apólice.

Atingido o limite de 10%, a PREVCOM poderá, a seu critério, rescindir o contrato e aplicar cumulativamente a multa compensatória prevista no item 9.2.3.

9.2.3. Multa compensatória

Aplicável nos casos de inexecução parcial ou total do objeto contratual, nos seguintes percentuais calculados sobre o valor do prêmio anual da apólice:

Hipótese	Percentual
Inexecução parcial — descumprimento de obrigação acessória com impacto na cobertura	5%
Inexecução parcial — recusa injustificada de acionamento de cobertura contratada	15%
Inexecução parcial — cancelamento unilateral de cobertura sem anuência da PREVCOM	20%
Inexecução total — rescisão por culpa da contratada ou recusa de emissão da apólice	30%

A multa compensatória não exclui a obrigação de reparar os danos causados à PREVCOM, podendo ser cobrada cumulativamente com perdas e danos apurados.

9.2.4. Impedimento de licitar e contratar

Aplicável pelo prazo de até 3 (três) anos, nos casos previstos no art. 156, III, da Lei nº 14.133/2021, incluindo:

- a) apresentação de documentação falsa ou declaração inverídica;
- b) fraude na execução do contrato;
- c) comportamento inidôneo ou embaraço à fiscalização.

9.2.5. Declaração de inidoneidade

Aplicável pelo prazo mínimo de 3 (três) anos e máximo de 6 (seis) anos, nos casos de maior gravidade previstos no art. 156, IV, da Lei nº 14.133/2021, incluindo atos lesivos à administração pública praticados em benefício da contratada.

9.2.6. Disposições gerais sobre sanções

- a) As sanções dos itens 9.2.2 e 9.2.3 poderão ser aplicadas cumulativamente entre si e com as sanções dos itens 9.2.4 e 9.2.5;
- b) É assegurado à contratada o direito ao contraditório e à ampla defesa no prazo de 15 (quinze) dias úteis, contados da notificação, antes da aplicação de qualquer sanção;
- c) Os valores de multa poderão ser descontados de eventuais créditos da contratada perante a PREVCOM ou cobrados judicialmente, caso insuficientes;
- d) A reincidência em infração já sancionada com advertência ensejará a aplicação da multa moratória ou compensatória correspondente, conforme a natureza do fato.

9.3. Retenção e glosa

A Contratante poderá realizar retenção ou glosa nos casos de: inexecução parcial, descumprimento de prazos, prestação em desconformidade com as especificações contratadas, falta de entrega de relatórios e aplicação de multas contratuais.

10. CRITÉRIOS DE MEDIÇÃO E DE PAGAMENTO

Recebimento

10.1. A apólice será recebida provisoriamente, de forma sumária, no ato de seu envio, juntamente com a nota fiscal ou instrumento de cobrança equivalente, pelo responsável pelo acompanhamento e fiscalização do contrato, para efeito de posterior verificação de sua conformidade com as especificações constantes neste Termo de Referência e na proposta da Contratada.

10.2. A apólice poderá ser rejeitada, no todo ou em parte, inclusive antes do recebimento provisório, quando estiver em desacordo com as especificações constantes neste Termo de Referência e na proposta, devendo ser substituída no prazo de 5 (cinco) dias úteis, contados da notificação da Contratada, às suas expensas, sem prejuízo da aplicação das penalidades cabíveis.

10.3. O recebimento definitivo ocorrerá no prazo de até 5 (cinco) dias úteis, contados do recebimento da nota fiscal ou instrumento de cobrança equivalente pela CONTRATANTE, após a verificação das informações e coberturas contratadas e consequente aceitação mediante termo detalhado.

10.4. O prazo para recebimento definitivo poderá ser excepcionalmente prorrogado, de forma justificada, por igual período, quando houver necessidade de diligências para aferição do atendimento das exigências contratuais.

10.5. No caso de controvérsia sobre a execução do objeto quanto à extensão da cobertura, às condições contratadas ou a quaisquer outros aspectos relacionados à apólice, havendo parcela incontroversa, deverá ser observado o disposto no art. 143 da Lei nº 14.133, de 2021, com a comunicação à Contratada para emissão da Nota Fiscal/Fatura correspondente à parcela incontroversa, para fins de liquidação e pagamento.

10.6. O prazo para a solução, pela Contratada, de inconsistências na execução do objeto ou para saneamento da nota fiscal ou de instrumento de cobrança equivalente, verificadas pela CONTRATANTE durante a análise prévia à liquidação da despesa, não será computado para fins de recebimento definitivo.

10.7. O recebimento provisório ou definitivo não excluirá a responsabilidade civil da Contratada

nem sua responsabilidade profissional pela perfeita execução do contrato, observadas as disposições legais aplicáveis.

Prazo de pagamento

10.8. O pagamento será efetuado no prazo de até 30 (trinta) dias, contados da apresentação da nota fiscal ou documento de cobrança equivalente.

10.9. No caso de atraso imputável à CONTRATANTE, os valores devidos à Contratada serão atualizados monetariamente na forma da legislação aplicável, incidindo, ainda, juros moratórios à razão de 0,5% (meio por cento) ao mês, calculados pro rata temporis sobre o período de atraso.

Forma de pagamento

10.10. O pagamento será realizado em parcela única, por meio de ordem bancária, para depósito em conta corrente de titularidade da Contratada, mantida no Banco do Brasil S.A.

10.10.1. Constitui condição para a realização dos pagamentos a inexistência de registros em nome da Contratada no Cadastro Informativo dos Créditos não Quitados de Órgãos e Entidades Estaduais – CADIN ESTADUAL, o qual deverá ser consultado por ocasião de cada pagamento. O cumprimento desta condição poderá ocorrer mediante comprovação, pela Contratada, de que os registros existentes se encontram suspensos, nos termos do art. 8º da Lei Estadual nº 12.799, de 2008.

10.11. Será considerada como data do pagamento o dia em que constar como emitida a ordem bancária correspondente.

10.12. O CONTRATANTE poderá, por ocasião do pagamento, efetuar as retenções tributárias previstas em lei, ainda que não haja indicação correspondente na nota fiscal apresentada ou que se refiram a retenções não realizadas em períodos anteriores.

10.12.1. Independentemente do percentual de tributo informado na planilha de composição de custos, quando aplicável, serão retidos na fonte os percentuais estabelecidos na legislação vigente.

10.13. A Contratada optante pelo Simples Nacional, nos termos da Lei Complementar nº 123, de 2006, não estará sujeita à retenção tributária dos impostos e contribuições abrangidos por esse regime. Contudo, o pagamento ficará condicionado à apresentação de documento oficial que comprove seu enquadramento e o direito ao tratamento tributário favorecido previsto na referida Lei Complementar.

10.14. É vedado o pagamento antecipado.

11. ESTIMATIVA DO VALOR E ADEQUAÇÃO ORÇAMENTÁRIA

11.1. O valor estimado da contratação tem caráter sigiloso e não será tornado público antes de definido o resultado do julgamento das propostas, nos termos do art. 24 da Lei nº 14.133/2021.

11.2. As despesas decorrentes da presente contratação correrão à conta de recursos próprios da Prevcom, consignados na dotação orçamentária nº 40201980200000000 do orçamento vigente, devidamente identificados na instrução do processo administrativo.

12. DISPOSIÇÕES FINAIS

12.1. A licitante deverá indicar endereço eletrônico oficial de comunicação em sua proposta, responsabilizando-se pelo efetivo recebimento das tratativas enviadas pela PREVCOM.

12.2. As licitantes assumem todos os custos de preparação e apresentação de suas propostas.

12.3. A Contratante poderá, a qualquer tempo, por despacho motivado, revogar o procedimento por razões de interesse público ou anulá-lo por ilegalidade, sem direito a indenização, conforme

art. 71 da Lei Federal nº 14.133/2021.

12.4. A contratação será formalizada mediante assinatura do instrumento contratual ou emissão de instrumento equivalente.

12.5. Fica eleito o Foro Cível da Comarca da Capital do Estado de São Paulo para dirimir quaisquer controvérsias decorrentes da presente contratação.

12.6. A apresentação da proposta implica a aceitação tácita de todas as disposições contidas no edital e em seus anexos.

ANEXO I -TERMO DE REFERÊNCIA PREVCOM Nº 034/2026

Processo SEI nº 271.00000513/2026-96

Objeto: contratação de apólice de seguro de riscos cibernéticos (“Seguro Cyber”), com cobertura ampla e especializada, voltada à proteção da Fundação de Previdência Complementar do Estado de São Paulo – PREVCOM contra impactos decorrentes de incidentes cibernéticos.

INFORMAÇÕES ADICIONAIS E PERFIL DE RISCO CIBERNÉTICO

1. Identificação do Proponente

1.1 Nome do Proponente:

Fundação de Previdência Complementar do Estado de São Paulo – SP-PREVCOM

1.2 CNPJ (Fundação):

15.401.381/0001-98

1.3 CNPJ dos Patrocinadores, por Plano de Benefícios:

PLANO DE BENEFÍCIOS PREVCOM RP

CNPJ	Patrocinador
46.379.400/0001-50	ESTADO DE SAO PAULO
63.025.530/0001-04	UNIVERSIDADE DE SAO PAULO
46.068.425/0001-33	UNIVERSIDADE ESTADUAL DE CAMPINAS
48.031.918/0001-24	UNIVERSIDADE ESTADUAL PAULISTA JULIO DE MESQUITA FILHO
59.952.259/0001-85	ASSEMBLEIA LEGISLATIVA DO ESTADO DE SAO PAULO
51.174.001/0001-93	TRIBUNAL DE JUSTICA DE SÃO PAULO
60.265.576/0001-02	TRIBUNAL DE JUSTICA MILITAR DO ESTADO DE SAO PAULO
01.468.760/0001-90	MINISTERIO PUBLICO DO ESTADO DE SAO PAULO
50.290.931/0001-40	TRIBUNAL DE CONTAS DO ESTADO SAO PAULO

08.036.157/0001-89	DEFENSORIA PUBLICA DO ESTADO DE SAO PAULO
--------------------	---

PLANO DE BENEFÍCIOS PREVCOM RG

CNPJ	Patrocinador
46.379.400/0001-50	ESTADO DE SAO PAULO
63.025.530/0001-04	UNIVERSIDADE DE SAO PAULO
46.068.425/0001-33	UNIVERSIDADE ESTADUAL DE CAMPINAS
48.031.918/0001-24	UNIVERSIDADE ESTADUAL PAULISTA JULIO DE MESQUITA FILHO
59.952.259/0001-85	ASSEMBLEIA LEGISLATIVA DO ESTADO DE SAO PAULO
51.174.001/0001-93	TRIBUNAL DE JUSTICA DE SÃO PAULO
60.265.576/0001-02	TRIBUNAL DE JUSTICA MILITAR DO ESTADO DE SAO PAULO
01.468.760/0001-90	MINISTERIO PUBLICO DO ESTADO DE SAO PAULO
50.290.931/0001-40	TRIBUNAL DE CONTAS DO ESTADO SAO PAULO
08.036.157/0001-89	DEFENSORIA PUBLICA DO ESTADO DE SAO PAULO

PLANO DE BENEFÍCIOS PREVCOM RG UNIS

CNPJ	Patrocinador
63.025.530/0001-04	UNIVERSIDADE DE SAO PAULO
46.068.425/0001-33	UNIVERSIDADE ESTADUAL DE CAMPINAS
48.031.918/0001-24	UNIVERSIDADE ESTADUAL PAULISTA JULIO DE MESQUITA FILHO

PLANO DE BENEFÍCIOS PREVCOM MULTI

CNPJ	Patrocinador
44.215.846/0001-14	ARARAS/SP
44.780.609/0001-04	BARRETOS/SP
46.151.718/0001-80	BIRIGUI/SP
44.435.121/0001-31	BURITAMA/SP
46.523.064/0001-78	CAIEIRAS/SP
53.307.906/0001-10	CAIUÁ/SP
46.179.958/0001-92	CÂNDIDO MOTA/SP
24.772.154/0001-60	CASTANHEIRA/MT
24.616.187/0001-10	DOIS IRMÃOS DO BURITI/MS

53.221.941/0001-11	FLOREAL/SP
18.307.439/0001-27	GUANHÃES/MG
03.239.019/0001-83	GUARANTÃ DO NORTE/MT
46.319.000/0001-50	GUARULHOS/SP
59.754.648/0001-04	ILHA SOLTEIRA/SP
46.523.130/0001-00	ITAPECERICA DA SERRA/SP
46.634.358/0001-77	ITAPEVA/SP
46.523.031/0001-28	ITAPEVI/SP
45.131.885/0001-04	JALES/SP
46.444.790/0001-03	JOÃO RAMALHO/SP
46.200.846/0001-76	LENÇÓIS PAULISTA/SP
46.363.933/0001-44	LOUVEIRA/SP
46.523.163/0001-50	MAIRIPORÃ/SP
45.353.307/0001-04	MIGUELÓPOLIS/SP
01.614.517/0001-33	NOVO MUNDO/MT
46.523.171/0001-04	OSASCO/SP
46.578.514/0001-20	PERUÍBE/SP
46.341.038/0001-29	PIRACICABA/SP
65.712.077/0001-30	PONTALINDA/SP
45.339.363/0001-94	PORTO FERREIRA/SP
44.723.757/0001-89	RAFARD/SP
01.612.911/0001-32	RESERVA DO IGUAÇU/PR
56.024.581/0001-56	RIBEIRÃO PRETO/SP
94.704.103/0001-86	RIO DOS ÍNDIOS/RS
45.135.043/0001-12	RUBINÉIA/SP
45.138.070/0001-49	SANTA FÉ DO SUL/SP
58.200.015/0001-83	SANTOS/SP
46.588.950/0001-80	SÃO JOSÉ DO RIO PRETO/SP
46.596.235/0001-99	SEVERÍNIA/SP
59.764.944/0001-88	SUZANÁPOLIS/SP
44.544.691/0001-15	TAIAÇU/SP
46.599.833/0001-11	VALENTIM GENTIL/SP
45.709.912/0001-75	VIRADOURO/SP

PLANO DE BENEFÍCIOS SP PREVIDÊNCIA

CNPJ	Patrocinador
------	--------------

46.395.000/0001-39	MUNICÍPIO DE SÃO PAULO
50.176.270/0001-26	TRIBUNAL DE CONTAS DO MUNICÍPIO DE SÃO PAULO
50.176.288/0001-28	CÂMARA MUNICIPAL DE SÃO PAULO

PLANO DE BENEFÍCIOS PREVCOM MS

CNPJ	Patrocinador
15.412.257/0001-28	ESTADO DE MATO GROSSO DO SUL

PLANO DE BENEFÍCIOS PREVCOM MT

CNPJ	Patrocinador
03.507.415/0001-44	ESTADO DE MATO GROSSO

PLANO DE BENEFÍCIOS PREVCOM PA

CNPJ	Patrocinador
05.054.861/0001-76	ESTADO DO PARÁ

PLANO DE BENEFÍCIOS PREVCOM RO

CNPJ	Patrocinador
00.394.585/0001-71	ESTADO DE RONDÔNIA

1.4 Endereço:

Av. Líbero Badaró, 377, 8º andar – Centro – São Paulo/SP – CEP 01009-906

1.5 Website:

www.prevcom.com.br

1.6 Data de início das atividades:

01/03/2012

1.7 Ramo de atividade:

Entidade Fechada de Previdência Complementar – EFPC

1.8 Quantidade de funcionários:

120

1.9 Distribuição geográfica:

Brasil: 100% | Exterior: 0% — sem sede ou subsidiárias nos EUA ou Canadá.

2. Informações Financeiras

2.1 Faturamento bruto / arrecadação (últimos 12 meses, mai/25 a abr/26):

R\$ 588.844.385,83

2.2 Expectativa para os próximos 12 meses (orçamento 2026):

R\$ 584.553.210,12

2.3 Total de ativos no balanço:

R\$ 5.472.175.621,00

3. Coberturas e Limites Pretendidos

3.1 Coberturas selecionadas:

- Responsabilidade Civil Cibernética
- Proteção por Interrupção de Rede
- Gestão de Incidentes
- Dados Eletrônicos
- Extorsão Cibernética

3.2 Limite de Indenização (LMG) pretendido:

R\$ 20.000.000,00

3.3 Divisão do LMG:

30% Custos de Defesa / 70% Indenizações

3.4 Importâncias seguradas pretendidas:

R\$ 20.000.000,00

4. Reclamações e Incidentes

- Reclamação, ação, investigação ou intervenção relacionada à violação de segurança/privacidade de dados nos últimos 5 anos: Não
- Conhecimento de reclamação ou circunstância que possa resultar em reclamação futura: Não
- Reclamação, ação ou investigação em andamento relacionada a incidentes cibernéticos ou notificação anterior em apólice de riscos cibernéticos: Não

5. Estrutura de Segurança da Informação

5.1 Responsável pela Segurança da Informação (CISO):

5.1.1. Participa das decisões estratégicas junto à alta administração:

Sim.

5.2 DPO formalmente designado:

Sim - Ana Flavia Cunha Canabrava

5.3 Venda de produtos online:

Não

5.4 Segurança da informação centralizada:

Sim. Centralizada na Diretoria de Tecnologia da Informação, com responsável/função de Segurança da Informação. SOC dedicado 24x7 em formação.

5.5 Revisão dos riscos cibernéticos pela alta administração (ao menos anual):

Parcial. Riscos e controles são tratados em governança, políticas e contratações; auditoria externa anual ainda não estabilizada.

5.6 Revisão da política de segurança por entidade externa:

Não há revisão periódica externa estabilizada; houve revisões pontuais por áreas internas e consultorias em projetos específicos.

5.7 Frameworks adotados:

ISO/IEC 27001, ISO/IEC 27002, LGPD; NIST e COBIT quando aplicável (boas práticas).

5.8 Certificação ISO 27001 / relatório SOC 2:

Não possui. Há iniciativa de adequação/maturidade em curso para ISO 27001.

5.9 Certificação PCI-DSS:

Não aplicável — não armazena/processa dados de cartão de crédito em ambiente próprio.

6. Gestão de Ativos de *Hardware* e *Software*

Existe inventário de ativos e sistemas, com atualização pelo menos anual (CyberEdge: ao menos duas vezes ao ano) e gestão centralizada pela DTI. Descoberta automatizada semanal de ativos ainda não está formalmente estabilizada.

Inventário de Ativos Críticos: Sim, com priorização conforme impacto no negócio/continuidade. Atualização periódica do inventário de dados sensíveis: ao menos anual.

7. Continuidade de Negócios, Backup e Recuperação

7.1 Objetivo de Tempo de Retorno (RTO) para Ativos Críticos:

Entre 1 e 7 dias.

7.2 Plano de Continuidade de Negócios (PCN):

Sim, existente.

7.3 Plano de Recuperação de Desastres (DRP):

Em maturação/implantação. Política documentada de recuperação de desastres: Sim, com padrões de backup conforme criticidade da informação.

7.4 Testes de restauração:

Trimestrais (conforme RTO definido), com testes adicionais sob demanda.

7.5 Estratégia de backup:

- Backup offline (archive) armazenado onsite: Não
- Backup regular armazenado onsite: Não
- Backup completo mensal e incremental diário, com armazenamento em nuvem/offsite: Sim
- Backups offline armazenados offsite / isolados do domínio de produção (imutáveis): Sim

7.6 Criptografia:

Full disk encryption obrigatório em dispositivos do usuário final com dados sensíveis: Sim. Criptografia em trânsito e em mídias móveis quando aplicável; criptografia em repouso depende do sistema/serviço contratado.

7.7 Classificação de dados sensíveis:

Sim, em fase de implantação/divulgação, alinhada à LGPD.

8. Gerenciamento de Identidades, Credenciais e Acessos

Diretório e Identidade

- Ferramentas em uso: Microsoft Active Directory, Azure Active Directory e Google Workspace
- Fonte principal de identidade para a maioria dos usuários: Microsoft Active Directory (autoridade/privilegios majoritariamente no AD); Microsoft 365 gerido por parceiro/Prodesp

Inventário e Validação de Credenciais

- Inventário com nomes, usuários, datas de início/fim de acesso e departamento: Sim
- Validação anual da autorização das credenciais existentes: Sim (validação trimestral não confirmada)

Política de Senhas

- Educação contra reutilização de senhas e política formal: Sim
- Solução para impedir senhas comuns/vazadas: Sim
- Gerenciador corporativo de senhas para funcionários: Não
- Microsoft LAPS ou equivalente para contas locais administrativas: Não formalizado

Autenticação Multifator (MFA)

- MFA para credenciais privilegiadas/Domain Admin: Sim (exigida)
- MFA para acesso remoto de funcionários: Parcial — implantada para alguns recursos corporativos, não todos
- MFA para acesso remoto de prestadores de serviço: Parcial — mesma situação dos funcionários
- MFA para Sistemas Críticos SaaS/terceiros: Parcial — alguns sistemas, não todos
- Nível de autenticação (AAL): AAL2 (para acessos com MFA; classificação ainda parcial)

Acessos Privilegiados

- PAM / cofre de senhas com rotação automática e gravação de sessão: Não implementado
- Estações de Trabalho Privilegiadas (PAW): Não
- Fluxo formal de aprovação time-bound para tarefas privilegiadas: Não
- Separação entre conta administrativa e conta de uso diário: Parcial
- Logs de uso de contas privilegiadas mantidos por ao menos 30 dias: Limitado/não confirmado

Controle de Acesso a Estações de Trabalho e Servidores

- Alguns usuários técnicos possuem privilégios de administrador local em estações de trabalho, conforme necessidade operacional
- Alguns usuários técnicos possuem privilégios administrativos em servidores para suporte/administração

9. Contas Privilegiadas — Quantitativos

Cód.	Questão / Resposta selecionada	Status
Domain Admins	Número de contas Domain Admin (contas em uso, ativas, agregadas em todos os domínios/florestas)	120
Contas de Serviço Privilegiadas	Número de Contas de Serviço Privilegiadas	7
Usuários Privilegiados	Usuários com credenciais de acesso privilegiado persistente para endpoints (estações/servidores)	7

- Inventário das contas de serviço privilegiadas, atualizado ao menos trimestralmente: Sim
- Rotação trimestral de senhas das contas de serviço privilegiadas: Sim
- Senhas mínimas de 25 caracteres para contas de serviço: Não
- Revisão anual dos privilégios/necessidade de cada conta de serviço: Não confirmado

10. Monitoramento de Segurança e Resposta a Incidentes

- Security Operations Center (SOC): Não possui equipe dedicada / SOC 24x7;
- SIEM consolidado: Não
- Logs centralizados / consumo de logs dos Controladores de Domínio via SIEM: Não
- DLP (Data Loss Prevention) em block mode ou não: Não
- Tempo médio de detecção e contenção de incidentes em estações de trabalho: Não medido

- Percentual de Ativos Críticos com logs enviados a SIEM / tempo de retenção: Não aplicável (sem SIEM)
- Ferramenta de simulação de ataques (BAS) ou red team interno: Não possui; testes externos podem ser contratados pontualmente
- Scan de vulnerabilidades para Ativos Críticos: Não
- Políticas de auditoria habilitadas nos Controladores de Domínio: Não possui

11. Resposta a Incidentes e *Phishing*

- Plano de resposta a incidentes documentado: Sim
- Plano inclui contato com polícia/órgãos reguladores após confirmação do incidente: Sim
- Plano inclui processo de retomada da operação via restauração de backups limpos: Sim
- Plano com procedimentos específicos para ransomware (organização e provedores de serviço): Não confirmado
- Processo documentado para resposta a incidentes de Phishing: Não
- Treinamento de conscientização de segurança aos funcionários (ao menos anual): Sim
- Simulações de ataques de Phishing para testar conscientização dos funcionários: Não confirmado

12. Gestão de Riscos e Aplicação de Patches

- Processo para gerenciar e instalar patches em todos os sistemas de TI, incluindo dispositivos portáteis: Sim
- SLA formal definindo prazos para aplicação de patches críticos: Não definido
- Percentual de compliance com padrões de deploy de patches críticos (último trimestre): Não medido
- Política de Uso Aceitável (AUP) descrevendo obrigações dos usuários: Sim
- Programa para lidar com ameaças internas e monitorar comportamentos de risco: Não confirmado

São Paulo, na data da assinatura digital.

Diego Galdino dos Santos
Assessor de Tecnologia da Informação

Alessandro Roosevelt Silva Riberio
Diretor de Tecnologia da Informação



A autenticidade deste documento pode ser conferida no site

[https://sei.sp.gov.br/sei/controlador_externo.php?](https://sei.sp.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0)

[acao=documento_conferir&id_orgao_acesso_externo=0](https://sei.sp.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0) , informando o código verificador **0114592273** e o código CRC **733C5A31**.