DIÁRIO OFICIAL DO ESTADO DE SÃO PAULO
Publicado na Edição de 28 de maio de 2026 | Caderno Executivo | Seção Atos Normativos

DELIBERAÇÃO DIRETORIA EXECUTIVA Nº 06, DE 8 DE MAIO DE 2026

Deliberação Diretoria Executiva nº 06, de 8 de Maio De 2026

Política de Segurança da Informação

DELIBERAÇÃO DIREX Nº 06/2026

Assunto: Aprova a Política de Segurança da Informação da Fundação de Previdência Complementar do Estado de São Paulo – SP-PREVCOM

A Diretoria Executiva da Fundação de Previdência Complementar do Estado de São Paulo – PREVCOM, em sua **697ª Reunião Ordinária**, realizada em **8 de maio de 2026**, por unanimidade, resolve:

Artigo 1º. Fica aprovado a Política de Segurança da Informação da Fundação de Previdência Complementar do Estado de São Paulo – PREVCOM, na forma do Anexo, que integra esta Deliberação para todos os fins.

Parágrafo único. Nos termos dos itens 2.2 e 2.3 da Política Interna de Elaboração e Gestão de Normativos da Prevcom este documento é classificado internamente como Regulamento.

Artigo 2º. Fica revogada a Política de Segurança da Informação aprovada pela Diretoria Executiva em 24 de fevereiro de 2021, bem como suas alterações posteriores.

Artigo 3º. Esta Deliberação entra em vigor na data de sua publicação.

SUMÁRIO

1. OBJETIVO

1.1. Esta Política de Segurança da Informação é uma declaração formal da Prevcom acerca de seu compromisso com a proteção das informações de sua propriedade e/ou sob sua guarda, devendo ser cumprida por todos os seus empregados, fornecedores, clientes e parceiros.

1.2. Seu objetivo é estabelecer as diretrizes a serem seguidas pelas partes envolvidas no que diz respeito à adoção de procedimentos, requisitos legais e práticas aplicadas, visando manter o alinhamento da Segurança da Informação com a estratégia organizacional e as recomendações dos Órgãos Reguladores, disseminando a importância e induzindo a melhoria contínua, promovendo a proteção dos dados pessoais e das informações sensíveis, propondo normas para o processo de gestão da Segurança da Informação.

2. ABRANGÊNCIA

2.1. As diretrizes aqui estabelecidas devem ser seguidas por todos os empregados, prestadores de serviço, agentes públicos e parceiros onde se aplicam à informação em qualquer meio ou suporte.

2.2. Esta política dá ciência a todas as partes interessadas de que os documentos, ambientes, sistemas, computadores e redes da empresa podem ser monitorados e gravados, com prévia informação, conforme previsto nas leis brasileiras.

2.3. É também obrigação de todos manter-se atualizado em relação a este documento, aos procedimentos e normas relacionadas.

2.4. A divulgação e distribuição da Política de Segurança da Informação é de responsabilidade da Diretoria de Tecnologia da Informação.

3. REFERÊNCIAS

3.1. Código de Conduta de Empregados;

3.2. LGPD - Lei nº 13.709, de 14 de agosto de 2018;

3.3. Norma ISO 27001:2022 - Sistema de Gestão de Segurança da Informação;

3.4. NIST SP 800-161 Rev. 1 - Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations.

3.5. Incidentes de segurança com dados pessoais: Grupo de Trabalho Ad Hoc DPOs das EFPCs. -- São Paulo: ABRAPP Associação Brasileira das Entidades Fechadas de Previdência Complementar, 2021.

4. DEFINIÇÕES

4.1. Terceiros - pessoas físicas ou jurídicas que tenham acesso a informações, sistemas, ativos de informação ou ambientes da Entidade, incluindo, entre outros, prestadores de serviços, fornecedores, consultores, auditores e parceiros institucionais.

4.2. Partes Interessadas - indivíduos, grupos ou organizações que possam afetar, ser afetados ou perceber-se afetados pelas atividades, decisões ou desempenho da PREVCOM no que se refere à Segurança da Informação, incluindo participantes, assistidos, patrocinadores, empregados, conselheiros, órgãos de governança, órgãos reguladores e terceiros.

4.3. SGSI: Sistema de Gestão de Segurança da Informação.

4.4. Ativos de Informação - Qualquer informação ou recurso relacionado à informação que tenha valor para a organização.

4.5. Melhoria Contínua - Processo incremental e constante de aperfeiçoamento das práticas e processos relacionados à segurança da informação.

4.6. Antivírus / Anti-malware – Programas destinados a prevenir, detectar e remover softwares maliciosos, como vírus, trojans, worms e spyware.

4.7. BitLocker – Ferramenta de criptografia da Microsoft para proteger dados em discos rígidos e unidades removíveis.

4.8. Black List – Lista de endereços de sites ou recursos bloqueados por apresentarem riscos de segurança ou conteúdo inapropriado.

4.9. Código-Fonte – Conjunto de instruções escritas em linguagem de programação que definem o funcionamento de um software.

4.10. Disponibilidade – Princípio da segurança que garante que a informação esteja acessível e utilizável por pessoas autorizadas sempre que necessário.

4.11. DLP (Data Loss Prevention) – Conjunto de ferramentas e políticas para prevenir perda, vazamento ou uso indevido de dados.

4.12. Firewall – Sistema que controla o tráfego de rede, filtrando conexões de entrada e saída conforme regras definidas.

4.13. HTTPS / TLS / SSL – Protocolos seguros de comunicação que utilizam criptografia para proteger dados transmitidos pela internet.

4.14. Malware – Qualquer software projetado para causar danos ou acessar sistemas de forma indevida.

4.15. Mensageiro Instantâneo (Instant Messaging) – Ferramenta para troca de mensagens em tempo real, como Microsoft Teams.

4.16. Protocolo de Segurança – Conjunto de regras e procedimentos usados para proteger dados e comunicações, aplicando métodos criptográficos.

4.17. TLS 1.2 ou Superior – Versão mínima recomendada do protocolo de criptografia Transport Layer Security para comunicações seguras.

4.18. Webmail – Interface para acessar e gerenciar e-mails por meio de um navegador web.

5. PRINCÍPIOS E DIRETRIZES

5.1. A utilização de recursos de informática deve ser feita de forma a preservar a segurança e integridade das informações e, para tanto, o usuário tem ciência da presente política e se obriga a segui-la com todo o rigor.

5.2. O acesso ao recurso disponibilizado para o usuário é estritamente necessário e indispensável ao exercício de suas atividades.

5.3. Princípios

5.4. A Segurança da Informação na PREVCOM é orientada por princípios que asseguram a proteção adequada das informações, a preservação da confiança institucional e a observância de valores éticos, legais e organizacionais, em alinhamento ao Sistema de Gestão da Segurança da Informação (SGSI).

5.5. Constituem princípios da Segurança da Informação na PREVCOM:

5.5.1. Confidencialidade: acesso às informações restrito às pessoas devidamente autorizadas, conforme suas atribuições e necessidades institucionais.

5.5.2. Integridade: exatidão, completude, consistência e confiabilidade das informações ao longo de todo o seu ciclo de vida.

5.5.3. Disponibilidade: acesso oportuno às informações e aos serviços necessários ao desempenho das atividades institucionais.

5.5.4. Confiança: relações institucionais seguras, previsíveis e transparentes com participantes, assistidos, patrocinadores, empregados, fornecedores e demais partes interessadas.

5.5.5. Legalidade: observância do ordenamento jurídico aplicável, das normas regulatórias e das diretrizes internas no uso, tratamento e proteção das informações.

5.5.6. Finalidade: utilização das informações limitada a propósitos institucionais legítimos, compatíveis com as atividades e objetivos da Entidade.

5.5.7. Necessidade: restrição do acesso, do uso e do compartilhamento das informações ao mínimo indispensável para a execução das atividades institucionais.

5.5.8. Transparência: clareza quanto às práticas de Segurança da Informação e aos procedimentos adotados no tratamento de incidentes relevantes, observado o sigilo quando aplicável.

5.5.9. Responsabilização: atribuição de responsabilidades claras aos agentes envolvidos no uso, no tratamento e na proteção das informações.

5.5.10. Prevenção: adoção de medidas destinadas a reduzir a probabilidade de ocorrência de incidentes de Segurança da Informação e a mitigar riscos identificados.

5.5.11. Proporcionalidade: compatibilidade entre os controles e medidas de Segurança da Informação e o nível de risco, impacto e criticidade das informações e processos envolvidos.

5.5.12. Continuidade: consideração da Segurança da Informação nos planos de continuidade do negócio e na recuperação de eventos adversos.

5.5.13. Prestação de Contas: rastreabilidade das decisões, ações e controles adotados no âmbito da Segurança da Informação.

5.5.14. Melhoria Contínua: aprimoramento permanente dos controles, processos e práticas de Segurança da Informação com base em riscos, incidentes, auditorias e revisões do SGSI.

5.5.15. Arquitetura e Engenharia de Sistemas Seguros: concepção, implementação e manutenção de sistemas, aplicações e infraestruturas com foco em segurança desde a concepção, gestão de riscos, prevenção de falhas e resiliência operacional.

5.5.16. Integração aos Processos Organizacionais: incorporação da Segurança da Informação aos processos de negócio, à governança e às decisões estratégicas da PREVCOM.

5.5.17. Suporte à Tomada de Decisão: produção de informações confiáveis, tempestivas e adequadas para subsidiar decisões institucionais.

5.6. Diretrizes

5.7. As diretrizes de Segurança da Informação da PREVCOM estabelecem orientações gerais para a proteção das informações, dos ativos informacionais e dos ambientes tecnológicos, devendo ser observadas por todos aqueles que, direta ou indiretamente, tenham acesso a informações ou sistemas da Entidade.

5.8. Constituem diretrizes de Segurança da Informação da PREVCOM:

5.8.1. Gestão de Riscos: identificação, análise, avaliação e tratamento de riscos de Segurança da Informação de forma contínua e integrada aos processos institucionais.

5.8.2. Controle de Acesso: concessão, manutenção e revogação de acessos às informações e aos sistemas com base no princípio do menor privilégio e na segregação de funções.

5.8.3. Uso Adequado dos Recursos: utilização dos recursos de tecnologia da informação de forma segura, responsável e compatível com as finalidades institucionais da PREVCOM.

5.8.4. Proteção das Informações: adoção de medidas destinadas a proteger as informações contra acesso não autorizado, divulgação indevida, alteração, perda ou destruição, ao longo de todo o seu ciclo de vida.

5.8.5. Segurança em Ambientes Tecnológicos: consideração de requisitos de Segurança da Informação na concepção, aquisição, desenvolvimento, operação e manutenção de sistemas, aplicações e infraestruturas tecnológicas.

5.8.6. Relação com Terceiros: observância de requisitos de Segurança da Informação na contratação, no acompanhamento e no encerramento de relações com fornecedores, prestadores de serviço e parceiros.

5.8.7. Comunicação e Tratamento de Incidentes: comunicação tempestiva e tratamento adequado de incidentes de Segurança da Informação, conforme procedimentos e planos específicos, inclusive o Plano de Resposta a Incidentes.

5.8.8. Continuidade do Negócio: integração da Segurança da Informação aos planos de continuidade do negócio, assegurando a resiliência institucional e a recuperação adequada em situações adversas.

5.8.9. Conscientização e Capacitação: promoção de ações de conscientização, orientação e capacitação em Segurança da Informação para os públicos internos e demais partes relevantes.

5.8.10. Conformidade e Monitoramento: monitoramento da conformidade com esta Política, com as normas internas e com os requisitos legais e regulatórios aplicáveis.

5.8.11. Registro e Rastreabilidade: manutenção de registros adequados das ações relevantes relacionadas à Segurança da Informação, assegurando rastreabilidade e prestação de contas.

5.8.12. Melhoria Contínua: revisão e aprimoramento contínuos das práticas, controles e diretrizes de Segurança da Informação, com base em riscos, incidentes, auditorias e análises críticas do SGSI.

6. PROCEDIMENTOS

6.1. Computador de Trabalho

6.1.1. Cada profissional receberá um computador de trabalho composta por hardware e software necessários às suas atividades.

6.1.2. O usuário é responsável pelas informações armazenadas localmente.

6.1.3. É obrigatório:

6.1.4. Bloquear o computador de trabalho ao se ausentar;

6.1.5. Desligar o equipamento ao final do expediente;

6.1.6. Manter apenas arquivos em uso na área de trabalho;

6.1.7. Utilizar diretórios corporativos para armazenamento;

6.1.8. É proibido:

6.1.9. Alterar configurações de hardware ou software sem autorização;

6.1.10. Copiar informações para mídias externas sem autorização;

6.1.11. Instalar softwares não homologados.

6.2. Equipamentos Pessoais e de Terceiros

6.2.1. É proibida a conexão de dispositivos pessoais à rede corporativa.

6.2.2. Será disponibilizada rede exclusiva para visitantes, com acesso apenas à internet, mediante cadastro e monitoramento.

6.3. Uso de Mídias Removíveis e Porta USB

6.3.1. A transferência de dados via USB é bloqueada por padrão.

6.3.2. A liberação ocorrerá apenas mediante:

6.3.3. Justificativa formal;

6.3.4. Aprovação do gestor;

6.4. Uso de dispositivo corporativo criptografado.

6.4.1. Todo tráfego será monitorado.

6.4.2. O usuário é responsável por eventuais impactos decorrentes do uso indevido.

6.5. Correio Eletrônico Corporativo

6.5.1. O e-mail corporativo é ferramenta exclusiva de trabalho.

6.5.2. As mensagens são de propriedade da Prevcom e podem ser auditadas.

6.5.3. É proibido:

6.5.4. Utilizar e-mail corporativo para fins pessoais (cadastros, compras, redes sociais).

6.5.5. Redirecionar e-mails para contas externas.

6.5.6. O cliente homologado é o Outlook institucional.

6.5.7. Assinaturas devem seguir padrão da Comunicação.

6.6. Compartilhamento e Transferência de Informações

6.6.1. A transferência formal de informações deve ocorrer via:

6.6.2. E-mail corporativo;

6.6.3. Microsoft Teams;

6.6.4. SEI;

6.6.5. Informações sigilosas devem ser criptografadas.

6.7. Armazenamento em Nuvem

6.7.1. Permitido apenas o uso do OneDrive corporativo.

6.7.2. Compartilhamento externo requer autorização do gestor.

6.7.3. Acessos deverão ser revogados ao término do vínculo.

6.8. Impressão

6.8.1. Impressoras são para uso profissional.

6.8.2. Impressões podem ser auditadas.

6.8.3. Documentos devem ser recolhidos imediatamente.

6.8.4. Impressões devem ser realizadas preferencialmente com recurso de impressão segura.

6.9. Telefonia

6.9.1. Uso restrito a atividades profissionais.

6.9.2. Ligações poderão ser gravadas em caso de suspeita de irregularidade.

6.10. Mensageria Instantânea

6.10.1. Permitido uso do Microsoft Teams corporativo.

6.10.2. Uso exclusivamente profissional.

6.10.3. Pode haver monitoramento.

6.11. Acesso à Internet

6.11.1. Acesso monitorado e registrado.

6.11.2. Proibido acesso a:

6.11.3. Conteúdo pornográfico;

6.11.4. Conteúdo racista;

6.11.5. Apologia a drogas ou violência;

6.11.6. Jogos;

6.11.7. Sites de apostas;

6.11.8. Sites maliciosos.

6.12. Uso de Software

6.12.1. Apenas softwares homologados podem ser instalados.

6.12.2. Instalações devem ser solicitadas à Infraestrutura.

6.13. Acesso Remoto

6.13.1. Permitido mediante controle da Infraestrutura.

6.14. Fornecedores somente com autorização formal e acompanhamento.

6.14.1. É vedado acesso remoto não monitorado.

6.15. Prevenção à Perda de Dados (DLP)

6.15.1. A ferramenta DLP será utilizada para:

6.15.2. Detectar vazamentos;

6.15.3. Monitorar tráfego de dados sensíveis;

6.15.4. Apoiar investigações.

6.16. Protocolos de Segurança

6.16.1. Novas implementações devem utilizar TLS 1.2 ou superior.

6.16.2. Protocolos inseguros devem ser descontinuados ou mitigados.

6.16.3. Dados pessoais e restritos devem ser criptografados.

6.17. Antivírus

6.17.1. Todos os equipamentos devem possuir antivírus corporativo ativo e atualizado.

6.17.2. Diretrizes detalhadas constam no Regulamento de Gestão de Vulnerabilidades.

6.18. Proteção da Informação

6.18.1. Informações devem ser utilizadas exclusivamente para fins autorizados.

6.18.2. É proibida divulgação não autorizada de informações confidenciais.

6.18.3. Incidentes devem ser reportados imediatamente.

6.19. Autenticação e Senhas

6.19.1. Senhas são pessoais e intransferíveis.

6.19.2. Requisitos mínimos:

6.19.3. caracteres;

6.19.4. Complexidade obrigatória;

6.19.5. Troca a cada 90 dias.

6.20. Acesso ao Código-Fonte

6.20.1. Controlado pela Gerência de TI, mediante perfil e necessidade.

6.21. Backup

6.21.1. Backup diário dos diretórios de rede.

6.21.2. Retenção: 30 dias.

6.21.3. Solicitações via Suporte Técnico.

6.22. Descarte Seguro

6.22.1. Mídias devem ser destruídas fisicamente ou sobrescritas.

6.22.2. Documentos impressos devem ser fragmentados.

6.23. REGISTRO DE INCIDENTES

6.23.1. Incidentes devem ser reportados ao canal oficial de Segurança da Informação ou Suporte Técnico.

6.23.2. Violações poderão resultar em:

6.23.3. Comunicação formal;

6.23.4. Advertência ou suspensão;

6.23.5. Demissão por justa causa, conforme art. 482 da CLT.

6.24. Os procedimentos técnicos, fluxos operacionais, especificações de ferramentas, padrões de configuração, critérios de monitoramento, rotinas de execução e demais orientações operacionais relacionadas à Segurança da Informação serão disciplinadas em documentos complementares, sem prejuízo da observância integral das disposições deste Regulamento.

6.25. Tais documentos complementares deverão estar formalmente aprovados pelas instâncias competentes, versionados, controlados e mantidos em repositório oficial da PREVCOM, observadas as diretrizes do Sistema de Gestão da Segurança da Informação (SGSI).

7. ESTRUTURA E FUNÇÕES

7.1. A execução deste Regulamento de Segurança da Informação observa a estrutura organizacional da PREVCOM, cabendo às unidades e aos cargos abaixo relacionados o cumprimento das atribuições necessárias à implementação, manutenção, monitoramento e melhoria contínua dos controles de segurança da informação.

7.2. Diretoria Executiva

a. assegurar o apoio institucional e a disponibilização dos recursos necessários à implementação do Sistema de Gestão de Segurança da Informação (SGSI);

b. deliberar sobre matérias estratégicas relacionadas à segurança da informação;

c. aplicar as medidas administrativas cabíveis em caso de descumprimento deste Regulamento.

7.3. Diretoria de Tecnologia da Informação (DTI)

a. coordenar a implementação e a manutenção dos controles técnicos e administrativos de segurança da informação;

b. garantir a confidencialidade, a integridade e a disponibilidade dos ativos de informação sob sua responsabilidade;

c. definir, implementar e monitorar mecanismos de controle de acesso, proteção de dados, gestão de vulnerabilidades, backup, continuidade e resposta a incidentes;

d. propor revisões e atualizações deste Regulamento, sempre que necessário.

e. executar as ações operacionais relacionadas à segurança da informação;

f. administrar perfis de acesso, autenticação e uso dos recursos tecnológicos;

g. monitorar eventos e incidentes de segurança da informação, adotando as providências cabíveis;

h. manter registros, evidências e relatórios relacionados à segurança da informação.

7.4. Gestores

a. assegurar que os empregados sob sua responsabilidade cumpram as disposições deste Regulamento;

b. avaliar e autorizar acessos a informações e sistemas, observados os princípios da necessidade e do menor privilégio;

c. comunicar à Diretoria de Tecnologia da Informação quaisquer riscos, incidentes ou não conformidades relacionadas à segurança da informação.

7.5. Empregados, Prestadores de Serviços e Agentes Públicos

a. cumprir integralmente as disposições deste Regulamento e dos normativos correlatos;

b. proteger as informações e os ativos de informação sob sua guarda ou acesso;

c. comunicar imediatamente qualquer incidente, suspeita de violação ou uso indevido de informações e recursos tecnológicos.

7.6. Área de Gestão de Riscos e Controles Internos

a. acompanhar a conformidade deste Regulamento com as políticas institucionais e a legislação aplicável;

b. apoiar a avaliação de riscos relacionados à segurança da informação;

c. recomendar melhorias e ajustes sempre que identificadas fragilidades ou não conformidades.

7.7. Terceiros e Partes Interessadas

a. observar e cumprir as disposições deste Regulamento e dos normativos de Segurança da Informação a ele correlatos, no que lhes for aplicável;

b. utilizar as informações, os sistemas e os ativos de informação da PREVCOM exclusivamente para as finalidades autorizadas;

c. adotar medidas de proteção compatíveis com os riscos associados às informações e aos acessos concedidos;

d. respeitar os limites de acesso, de uso e de compartilhamento das informações institucionais;

e. comunicar prontamente à PREVCOM qualquer incidente, suspeita de violação ou evento que possa comprometer a Segurança da Informação;

f. cooperar com a PREVCOM na prevenção, identificação e tratamento de incidentes de Segurança da Informação, quando aplicável.

8. PENALIDADES E MEDIDAS DISCIPLINARES

8.1. O descumprimento das disposições estabelecidas neste Regulamento e demais normativos de segurança da informação sujeitará os responsáveis à aplicação de penalidades e medidas disciplinares cabíveis, proporcionais à natureza e à gravidade da infração, à existência de dolo ou culpa, à reincidência, ao impacto institucional, bem como aos riscos e danos efetivos ou potenciais à segurança da informação da PREVCOM.

8.2. As medidas disciplinares poderão incluir, de forma não exaustiva, advertência, suspensão de acesso a recursos tecnológicos, bloqueio temporário ou definitivo de credenciais, responsabilização administrativa, contratual ou legal, sem prejuízo de outras sanções previstas na legislação vigente e nos normativos internos da Prevcom.

8.3. Sem prejuízo das medidas disciplinares, a PREVCOM poderá adotar ações imediatas de contenção e mitigação de riscos, incluindo a restrição ou revogação de acessos, bloqueio de dispositivos e isolamento de ativos comprometidos, com o objetivo de preservar a integridade, confidencialidade e disponibilidade das informações.

8.4. A apuração das irregularidades observará o devido processo legal, assegurando-se o contraditório e a ampla defesa, respeitando-se as competências das instâncias responsáveis, bem como os procedimentos internos de gestão de incidentes de segurança da informação.

9. REVISÃO E ATUALIZAÇÃO

9.1. Este Regulamento deverá ser revisada periodicamente, no mínimo a cada 02 (dois) anos, ou sempre que houver alterações relevantes no ambiente organizacional, nos processos institucionais, na legislação aplicável ou nas normas internas e externas relacionadas à segurança da informação e à proteção de dados observadas as instâncias competentes e o sistema normativo da PREVCOM.

9.2. A revisão poderá ser proposta pela Diretoria de Tecnologia da Informação, pela Área de Gestão de Riscos, Controles Internos e Conformidade, pela Assessoria Jurídica ou por determinação da Alta Administração, devendo ser submetida às instâncias competentes para aprovação, nos termos da Política Interna de Elaboração e Gestão de Normativos.

10. VIGÊNCIA

10.1. Este Regulamento entra em vigor na data de sua aprovação pela Diretoria Executiva, iniciando-se, a partir de então, o prazo de 60 (sessenta) dias corridos a título de vacatio legis, destinado ao conhecimento do normativo, à realização de ações de conscientização e à adequação dos processos internos e controles necessários ao seu integral cumprimento.

11. DISPOSIÇÕES FINAIS

11.1. Durante o período de vacatio legis, a Diretoria de Tecnologia da Informação deverá promover a divulgação do Regulamento, bem como orientar empregados, colaboradores e terceiros quanto às diretrizes estabelecidas, podendo ser adotadas medidas educativas e preventivas com vistas à plena conformidade.

11.2. Após o decurso do prazo estabelecido, o cumprimento das disposições deste Regulamento tornar-se-á obrigatório, sujeitando os responsáveis às penalidades e medidas disciplinares cabíveis, conforme previsto nos normativos internos da PREVCOM.