



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 07, DE 8 DE MAIO DE 2026

Deliberação Diretoria Executiva nº 07, de 8 de Maio de 2026

Política de Classificação da Informação

DELIBERAÇÃO DIREX Nº 07/2026

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**, resolve:

Artigo 1º. Fica aprovada a **Política de Classificação 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. Esta Deliberação entra em vigor na data de sua publicação.

SUMÁRIO

- 1.OBJETIVO
- 2.ABRANGÊNCIA
- 3.REFERÊNCIAS
- 4.DEFINIÇÕES
- 5.PRINCÍPIOS E DIRETRIZES
- 6.ESTRUTURA E FUNÇÕES
- 7.PROCEDIMENTOS
- 8.RESPONSABILIDADES
- 9.PENALIDADES E MEDIDAS DISCIPLINARES

10. REVISÃO E ATUALIZAÇÃO

11. VIGÊNCIA

12. DISPOSIÇÕES FINAIS

1. OBJETIVO

1.1. Esta Política tem por objetivo estabelecer as diretrizes para a classificação e o tratamento das informações e dados no âmbito da PREVCOM, de modo a assegurar sua adequada proteção durante todo o ciclo de vida, observando a confidencialidade, integridade e disponibilidade das informações, em alinhamento ao Sistema de Gestão da Segurança da Informação (SGSI) e ao sistema normativo institucional.

1.2. Visa, ainda, proteger as informações submetidas a restrições de acesso nos termos da Lei federal nº 12.527, de 18 de novembro de 2011, e do Decreto estadual nº 68.155/2023 de 9 de dezembro de 2023, por meio de critérios técnicos e objetivos, observando o uso da medida menos restritiva possível, tendo em vista a adoção da publicidade como preceito geral e do sigilo como exceção, conforme previsto na Lei de Acesso à Informação ("LAI").

1.3. A classificação deverá orientar a definição de controles e medidas de segurança proporcionais ao nível de sensibilidade e ao impacto potencial decorrente de acesso não autorizado, alteração indevida ou indisponibilidade, garantindo o uso adequado, a proteção e o compartilhamento responsável das informações, conforme as normas internas e os requisitos aplicáveis.

2. ABRANGÊNCIA

2.1. As diretrizes desta Política devem ser aplicadas em todos os dados e informações, em qualquer meio (físico ou digital), tratados por colaboradores, conselheiros, membros de comitês, dirigentes, prestadores de serviço e quaisquer terceiros com acesso à informação da PREVCOM.

3. REFERÊNCIAS

3.1. Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação – LAI), que dispõe sobre o acesso a informações.

3.2. Decreto nº 68.155, de 09 de dezembro de 2023, que regulamenta, em âmbito estadual, a Lei federal nº 12.527, de 18 de novembro de 2011.

3.3. Lei nº 13.709, de 14 de agosto de 2018 – Lei Geral de proteção de Dados (LGPD);

3.4. ISO/IEC 27001 – Sistemas de Gestão da Segurança da Informação (SGSI): norma internacional que estabelece requisitos para a implementação, manutenção e melhoria contínua de um sistema de gestão da segurança da informação, com foco na confidencialidade, integridade e disponibilidade das informações.

3.5. NIST SP 800-161 Práticas de Gestão de Riscos de Cibersegurança na Cadeia de Suprimentos para Sistemas e Organizações, que fornece diretrizes para identificar, avaliar e mitigar riscos de segurança da informação associados à cadeia de suprimentos de tecnologia da informação.

3.6.Regulamento - Política Interna de Elaboração e Gestão de Normativos

3.7.Regulamento - Política de Segurança da Informação

3.8.Código de Ética e Conduta

3.9.Regulamento - Política de Privacidade

4.DEFINIÇÕES

4.1.Ativos da informação: recursos que contêm dados e informações e incluem, mas não se limitam a:

4.2.Documentos: relatórios, contratos, políticas e procedimentos;

4.3.Dados Digitais: bancos de dados, arquivos eletrônicos, e-mails.

4.4.Software: aplicativos e sistemas que processam e armazenam informações.

4.5.Hardware: equipamentos físicos como servidores, computadores e dispositivos de armazenamento.

4.6.Classificação da informação: atribuição de grau de sigilo a informações nos termos da Lei nº 12.527/2011.

4.7.Dado pessoal: qualquer informação que permite identificar, direta ou indiretamente, uma pessoa natural. Exemplos incluem nome e sobrenome; data de nascimento; RG; CPF; endereço residencial e de e-mail; número de telefone; dados bancários; dados de localização (como GPS); endereço de IP, entre outros.

4.8.Dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

4.9.Documento: toda informação produzida que seja registrada ou recebida em qualquer formato.

4.10.Informação: dados, processados ou não, que podem ser utilizados para a produção e a transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;

4.11.Informação pessoal: aquela relacionada à pessoa natural identificada ou identificável.

4.12.Informação pública: informação cujo acesso é franqueado ao público em geral, nos termos da Lei de Acesso à Informação, não estando sujeita a restrições de sigilo ou controle especial de acesso.

4.13.Informação de acesso restrito: informação com acesso permitido limitado a um grupo específico de pessoas.

4.14. Informação sigilosa: informação submetida, por tempo determinado, à restrição de acesso do público.

4.15. Informação classificada em grau de sigilo: informação sigilosa em poder dos órgãos e entidades públicas, observado o seu teor e em razão de sua imprescindibilidade à segurança da sociedade ou do Estado, classificada como ultrassecreta, secreta ou reservada conforme procedimentos específicos de classificação estabelecidos na LAI;

4.16. Tratamento da informação: toda ação referente à produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle da informação.

5. PRINCÍPIOS E DIRETRIZES

5.1. Princípios

5.1.1. A classificação das informações será orientada pelos seguintes princípios:

5.1.2. Confidencialidade: proteção das informações contra acesso, uso ou divulgação não autorizados, conforme o nível de classificação atribuído.

5.1.3. Integridade: preservação da exatidão, completude e confiabilidade das informações, prevenindo alterações indevidas ou não autorizadas.

5.1.4. Disponibilidade: garantia de que as informações estejam acessíveis sempre que necessárias ao desempenho das atividades institucionais.

5.1.5. Finalidade: utilização das informações exclusivamente para finalidades institucionais legítimas e compatíveis com as atribuições da PREVCOM.

5.1.6. Necessidade: limitação do acesso e do uso das informações ao mínimo indispensável para a execução das atividades institucionais.

5.1.7. Proporcionalidade: adoção de controles e medidas de proteção compatíveis com o nível de sensibilidade da informação e com o impacto potencial decorrente de sua exposição, alteração ou indisponibilidade.

5.1.8. Responsabilização: atribuição clara de responsabilidades quanto à classificação, ao uso, ao armazenamento, ao compartilhamento e à proteção das informações.

5.1.9. Transparência: clareza quanto aos critérios de classificação e às diretrizes aplicáveis, observados os limites legais e normativos de sigilo.

5.2. Diretrizes

5.2.1. De acordo com a ISO/IEC 27001, classificar a informação visa assegurar-lhe o nível adequado de proteção, como forma de mitigar o acesso indevido por falta de conhecimento do tipo de dado que se encontra disponível.

5.2.2.A classificação das informações na PREVCOM observará princípios e diretrizes destinados a assegurar a proteção adequada dos dados e informações ao longo de todo o seu ciclo de vida, em consonância com o Sistema de Gestão da Segurança da Informação (SGSI), o sistema normativo institucional e as boas práticas de Segurança da Informação.

5.2.3.Assim, as informações de propriedade da PREVCOM ou sob sua responsabilidade deverão ser classificadas de acordo com seu valor, criticidade, sensibilidade e sigilo, além da observância a requisitos legais, nas seguintes categorias:

5.2.3.1. Públicas: informações disponíveis à divulgação ao público interno e externo da PREVCOM, sem a aplicação de restrições e de controle de acesso.

5.2.3.2. Restritas: informações submetidas à limitação de acesso em razão de seu grau de sigilo protegido legalmente, as quais, se indevidamente publicadas, poderão acarretar impactos graves à Fundação e seus participantes.

5.2.3.3. Sigilosa: Informações temporariamente submetidas à restrição de acesso por serem imprescindíveis à segurança da sociedade ou do Estado, conforme graus e prazos definidos na LAI.

5.3.Considerando a natureza de suas atividades, a PREVCOM não produz informações classificadas nos graus reservado, secreto ou ultrassecreto.

5.4.Todo documento deverá apresentar, de forma clara e visível, no cabeçalho ou rodapé, o respectivo nível de classificação.

5.5.As informações produzidas, manuseadas e guardadas pela PREVCOM devem ser de acesso público, e sua restrição de acesso deve ser realizada em casos específicos, em conformidade com o previsto na LAI, que define que o acesso público é a regra e, o sigilo, a exceção.

5.6.A classificação de informação como restrita deverá se dar apenas mediante o enquadramento em uma hipótese legal. Para esse fim, e tendo em vista que a PREVCOM utiliza o Sistema Eletrônico de Informações (SEI), que é a plataforma do Governo do Estado de São Paulo para produção e gestão de documentos e processos administrativos, para enquadramento em grau de restrição deverão ser utilizadas as hipóteses legais elencadas no SEI.

5.7.O nível de classificação da informação deverá orientar a definição e a aplicação de controles de acesso físicos e lógicos.

5.8.A classificação das informações deverá ser revista sempre que houver mudança relevante em seu conteúdo, finalidade, contexto de uso ou grau de sensibilidade.

6. ESTRUTURA E FUNÇÕES

6.1.A estrutura organizacional relacionada à execução desta Política de Classificação de Dados compreende as instâncias de governança, as unidades administrativas e os agentes internos e externos que, direta ou indiretamente, produzem, tratam, armazenam, acessam ou gerenciam informações de propriedade ou sob a responsabilidade da Fundação de Previdência Complementar do Estado de São Paulo – PREVCOM.

6.2.A **Alta Administração**, representada pela Diretoria Executiva, é responsável pela aprovação, revisão periódica e patrocínio institucional desta Política, bem como pela garantia da disponibilização dos recursos necessários à sua implementação e à promoção da cultura organizacional voltada à segurança da informação e à proteção de dados.

6.3.A **Diretoria de Tecnologia da Informação** é a unidade responsável pela proposição, coordenação e manutenção desta Política, competindo-lhe estabelecer diretrizes técnicas, apoiar sua aplicação, promover ações de conscientização, monitorar o cumprimento das disposições estabelecidas e apoiar a realização de auditorias e avaliações periódicas.

6.4.A função de **Segurança da Informação** é responsável por orientar os colaboradores quanto à correta classificação, uso e proteção das informações, bem como por acompanhar a aderência aos controles de segurança aplicáveis, em consonância com o Sistema de Gestão de Segurança da Informação – SGSI.

6.5.O **Encarregado de Proteção de Dados (DPO)** atua de forma independente e transversal, prestando orientações relativas ao tratamento de dados pessoais e dados pessoais sensíveis, zelando pela conformidade com a Lei Geral de Proteção de Dados e apoiando a Fundação no relacionamento com titulares de dados e autoridades competentes.

6.6.As **Áreas** e seus respectivos gestores são responsáveis pela correta classificação das informações sob sua gestão, pela observância das diretrizes desta Política no âmbito de suas atividades e pela adoção de medidas necessárias à proteção, armazenamento e descarte adequado dos dados e documentos produzidos ou tratados.

6.7.Os **Empregados e Membros de Órgãos Estatutários** devem cumprir integralmente as disposições desta Política, classificando adequadamente as informações no momento de sua criação ou alteração, utilizando-as exclusivamente para finalidades institucionais autorizadas e protegendo-as contra acessos, usos, modificações ou divulgações não autorizadas.

6.8.Os **Prestadores de serviços, fornecedores e parceiros** que, no exercício de atividades contratadas ou parcerias institucionais, tratem dados ou informações de propriedade ou sob a guarda da PREVCOM, estão vinculados ao cumprimento das diretrizes desta Política, devendo observar as normas internas de segurança da informação e proteção de dados, conforme estabelecido em instrumentos contratuais, termos de confidencialidade ou documentos equivalentes.

7.PROCEDIMENTOS

7.1.Armazenamento

7.1.1.A aplicação da classificação das informações na PREVCOM será realizada por meio de procedimentos operacionais específicos, definidos, mantidos e atualizados em instrumentos normativos complementares, observadas as diretrizes desta Política e do Sistema de Gestão da Segurança da Informação (SGSI).

7.2.Os procedimentos deverão contemplar, no mínimo:

a.a atribuição da classificação da informação no momento de sua criação, recebimento ou coleta, ou tão logo seja incorporada aos processos institucionais;

b.a identificação do responsável pela informação e pela manutenção de sua classificação;

c.a definição de controles de acesso, uso, armazenamento, compartilhamento, retenção e descarte compatíveis com o nível de classificação atribuído;

d.a revisão da classificação sempre que houver alteração relevante no conteúdo, na finalidade, no contexto de uso ou no grau de sensibilidade da informação;

e.o registro e a rastreabilidade das decisões relacionadas à classificação e ao tratamento das informações;

f. a integração da classificação da informação com os demais normativos institucionais aplicáveis, inclusive a Política de Segurança da Informação e a Política de Privacidade.

7.3. Os procedimentos operacionais poderão ser atualizados sempre que necessário, em razão de mudanças tecnológicas, normativas, regulatórias ou organizacionais, sem necessidade de revisão desta Política, desde que preservados seus princípios e diretrizes.

8.RESPONSABILIDADES

8.1.Empregados

8.2.Cumprir as regras estabelecidas nesta Política, incluindo:

a. assegurar a correta classificação dos documentos, dados ou informações no momento de sua criação ou alteração;

b. primar pelo correto manuseio e tratamento das informações sob sua responsabilidade de gestão e guarda;

c.assegurar que as informações, sistemas e recursos tecnológicos disponibilizados pela PREVCOM sejam utilizados apenas para as finalidades aprovadas;

d.consultar a gerência da área, o responsável pela Segurança da Informação ou o Encarregado de Proteção de Dados sempre que informações de uso interno ou restrito forem solicitadas por um agente externo ao grupo ao qual o acesso ao documento esteja restrito ou sempre que necessitar de orientação;

e.no âmbito de suas atribuições e responsabilidades, proteger a informação contra acesso, modificação, destruição ou divulgação não autorizados.

8.3.Diretoria de Tecnologia da Informação:

8.4.Deverá adotar mecanismos de controle e realizar auditorias periódicas, com o objetivo de verificar:

- a.a correta aplicação das categorias de classificação da informação
- b.a conformidade dos procedimentos de armazenamento, acesso e descarte;
- c.a aderência às normas legais, regulatórias e internas aplicáveis.
- d.promover o monitoramento periódico do cumprimento desta Política;
- e.propor e executar ações regulares de conscientização, incluindo treinamentos, campanhas educativas e envio de comunicados institucionais sobre classificação e proteção da informação.

8.5.Encarregado de Proteção de Dados:

- 8.5.1.Fornece orientações relativas ao tratamento de dados pessoais e dados pessoais sensíveis.

8.6.Altima Administração (Diretoria Executiva):

- 8.6.1.aprovar e promover a revisão periódica desta Política, nos termos da Política Interna de Elaboração e Gestão de Normativos;
- 8.6.2.assegurar a disponibilização dos recursos necessários à sua implementação, manutenção e aprimoramento;
- 8.6.3.apoiar e patrocinar ações de capacitação, treinamentos e conscientização em segurança da informação;
- 8.6.4.fomentar a cultura organizacional voltada à proteção da informação, à governança de dados e à conformidade legal.

8.7.Prestadores de serviço, fornecedores e parceiros:

- 8.7.1.Os terceiros que, no exercício de atividades contratadas ou parcerias institucionais, tratem dados e informações de propriedade ou sob a guarda da PREVCOM deverão observar integralmente as diretrizes desta Política, bem como as normas de segurança da informação e de proteção de dados pessoais da Fundação, devendo tal obrigação constar expressamente dos instrumentos contratuais e/ou termos de confidencialidade aplicáveis.
- 8.7.2.A PREVCOM deverá adotar mecanismos de controle e realizar auditorias periódicas, internas ou externas, com o objetivo de verificar:
 - a.a correta aplicação das categorias de classificação da informação;
 - b.a conformidade dos procedimentos de armazenamento, acesso e descarte;
 - c.a aderência às normas legais, regulatórias e internas aplicáveis.
- 8.7.3.Os resultados dessas avaliações poderão subsidiar ações de melhoria contínua, revisões desta Política e medidas corretivas ou preventivas.

9.PENALIDADES E MEDIDAS DISCIPLINARES

9.1.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.

9.2.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.

9.3.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.

9.4.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.

10.REVISÃO E ATUALIZAÇÃO

10.1.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.

10.2.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.

11.VIGÊNCIA

11.1.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.

12.DISPOSIÇÕES FINAIS

12.1.Durante o período de vacatio legis, a Diretoria 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.

12.2.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.