DIÁRIO OFICIAL DO ESTADO DE SÃO PAULO
Publicado na Edição de 8 de julho de 2026 | Caderno Executivo | Seção Atos Normativos

DELIBERAÇÃO DIREX Nº 11, DE 01 DE JULHO DE 2026

DELIBERAÇÃO DIREX Nº 11 DE 01 DE JULHO DE 2026

Assunto: Aprova a Política de Gestão de Vulnerabilidades 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 698ª Reunião Ordinária, realizada em 13 de maio de 2026, por unanimidade, resolve:

Artigo 1º. Fica aprovada a Política de Gestão de Vulnerabilidades 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.

POLÍTIA DE GESTÃO DE VULNERABILIDADES

SUMÁRIO

1. Objetivo

1.1. Estabelecer práticas de gestão de vulnerabilidades e avaliação de impacto capazes de prevenir proativamente a exploração de eventuais vulnerabilidades e a potencial perda, comprometimento ou exposição indevida de dados da PREVCOM.

1.2. A PREVCOM cria e documenta práticas para a gestão sistemática de vulnerabilidades técnicas e não técnicas que possam afetar a Segurança da Informação da PREVCOM, abrangendo ativos tecnológicos, processos, pessoas, terceiros e aspectos organizacionais, de modo a apoiar a prevenção de incidentes, a mitigação de riscos e a melhoria contínua do Sistema de Gestão de Segurança da Informação (SGSI).

2. Abrangência

2.1. Este Regulamento aplica-se a todos os empregados da PREVCOM, bem como aos terceiros que mantenham relação contratual ou institucional com a Entidade, no que couber.

3. Referências

3.1. Constituem referências deste Regulamento:

I. ABNT NBR ISO/IEC 27001:2022 – Sistemas de Gestão de Segurança da Informação – Requisitos;

II. ABNT NBR ISO/IEC 27002:2022 – Código de Prática para Controles de Segurança da Informação;

III. ABNT NBR ISO/IEC 27005:2019 – Gestão de Riscos de Segurança da Informação;

IV. ABNT NBR ISO 31000:2018 – Gestão de Riscos – Diretrizes;

V. ABNT NBR 16167:2020 – Classificação, rotulação e tratamento da informação;

VI. Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD);

VII. Política de Segurança da Informação da PREVCOM;

VIII. Política Interna de Elaboração e Gestão de Normativos, denominada Norma Zero.

4. Definições

4.1. Para fins deste Regulamento, aplicam-se as seguintes definições:

4.1.1. Vulnerabilidade: fragilidade ou falha em ativo, sistema, processo ou controle que pode ser explorada por uma ameaça.

4.1.2. Patch: atualização de software destinada a corrigir falhas de segurança ou funcionamento.

4.1.3. Endpoint: dispositivo final conectado à rede corporativa, como computadores, notebooks e dispositivos móveis.

4.1.4. Endpoint Protection: solução de segurança destinada à proteção de endpoints contra ameaças cibernéticas.

4.1.5. Pentest ou Teste de Penetração: simulação controlada de ataque com o objetivo de identificar vulnerabilidades em sistemas e redes.

4.1.6. SIEM: ferramenta de gerenciamento e correlação de eventos de segurança da informação.

5. Princípios e Diretrizes

5.1. Princípios

5.1.1. A gestão de vulnerabilidades da PREVCOM observará, dentre outros, os seguintes princípios:

I. Prevenção e atuação proativa na mitigação de riscos de segurança da informação;

II. Proteção da confidencialidade, integridade e disponibilidade das informações;

III. Conformidade com a legislação vigente e com normas técnicas aplicáveis;

IV. Transparência, rastreabilidade e responsabilidade na gestão de vulnerabilidades;

V. Melhoria contínua dos controles de segurança da informação;

VI. Proporcionalidade, de modo que os esforços de identificação, tratamento e mitigação de vulnerabilidades sejam compatíveis com a criticidade dos ativos, a relevância dos serviços afetados e o contexto organizacional;

VII. Abrangência, contemplando vulnerabilidades técnicas e não técnicas, incluindo aspectos tecnológicos, processuais, humanos, organizacionais e de terceiros.

5.2. Diretrizes

5.2.1. Processo de Gestão de Vulnerabilidades

5.2.1.1. A Gestão de Vulnerabilidades na PREVCOM será executada por meio de procedimentos operacionais mantidos e atualizados no âmbito do Sistema de Gestão de Segurança da Informação (SGSI), assegurando padronização, rastreabilidade e evidências suficientes para auditorias internas e externas.

5.2.1.2. Os procedimentos de Gestão de Vulnerabilidades deverão contemplar, no mínimo, as etapas previstas neste Regulamento, observadas as responsabilidades definidas e as normas complementares aplicáveis.

5.2.2. Identificação e Descoberta de Vulnerabilidades

5.2.2.1. A identificação de vulnerabilidades deverá abranger ativos, sistemas, aplicações, redes e serviços sob responsabilidade da PREVCOM, incluindo ambientes próprios e terceirizados, com base em fontes internas e externas, tais como:

I. Varreduras automatizadas e inventários de ativos;

II. Alertas de fornecedores, fabricantes e entidades de referência;

III. Registros de incidentes e eventos de segurança;

IV. Testes controlados, auditorias técnicas e avaliações periódicas;

V. Notificações de terceiros, usuários e partes interessadas.

5.2.2.2. Deverá ser mantido banco de dados de vulnerabilidades, alimentado por múltiplas fontes confiáveis, tais como boletins de segurança, publicações de fornecedores, bases especializadas e ferramentas de monitoramento aplicáveis aos sistemas e ativos de informação da PREVCOM.

5.2.3. Registro, Evidência e Rastreabilidade

5.2.3.1. Toda vulnerabilidade identificada deverá ser registrada em repositório oficial, denominado Banco de Dados de Vulnerabilidades, com informações mínimas que permitam rastreabilidade, tais como:

I. Identificação do ativo afetado e do responsável;

II. Descrição e fonte da vulnerabilidade;

III. Data e hora de identificação e registro;

IV. Classificação de criticidade e impacto;

V. Decisão de tratamento e plano de ação;

VI. Planos de correção e mitigação;

VII. Evidências de correção, mitigação ou aceite;

VIII. Data e hora de encerramento e validação.

5.2.3.2. O banco de dados deverá ser atualizado regularmente, de forma a refletir as informações mais recentes disponíveis, devendo novas vulnerabilidades ser registradas tempestivamente após sua identificação.

5.2.3.3. Sempre que possível, o banco de dados deverá ser integrado a ferramentas de segurança da informação, tais como scanners de vulnerabilidades, soluções de gerenciamento de patches e plataformas de monitoramento, com vistas a aumentar a eficiência na identificação e no tratamento das vulnerabilidades.

5.2.3.4. As informações consolidadas no banco de dados deverão ser analisadas periodicamente, com o objetivo de identificar tendências, padrões e recorrências, subsidiando a adoção de medidas

preventivas e o aprimoramento contínuo dos controles de segurança da informação.

5.2.4. Critérios de Classificação e Priorização

5.2.4.1. As vulnerabilidades deverão ser classificadas e priorizadas considerando, ao menos:

I. Severidade técnica, explorabilidade e existência ou facilidade de obtenção de códigos, ferramentas, scripts ou métodos conhecidos que permitam explorar a vulnerabilidade, aumentando a probabilidade de sua exploração efetiva;

II. Criticidade do ativo e do processo de negócio afetado;

III. Impacto potencial à confidencialidade, integridade e disponibilidade;

IV. Exposição, considerando internet, rede interna ou acesso privilegiado;

V. Existência de controles mitigatórios.

5.2.5. Tratamento de Vulnerabilidades

5.2.5.1. O tratamento de vulnerabilidades deverá adotar medidas proporcionais ao risco, com base em abordagem preventiva e priorização por criticidade, visando reduzir ou eliminar o potencial de exploração e evitar a ocorrência de incidentes de segurança da informação.

5.2.5.2. O tratamento poderá incluir, entre outras medidas:

I. Correção, por meio de patch, atualização ou ajuste de configuração;

II. Mitigação por meio de controles compensatórios;

III. Isolamento ou restrição de exposição do ativo;

IV. Descontinuidade controlada de serviço ou ativo, quando necessário;

V. Aceite de risco residual, quando aplicável, conforme a governança de riscos.

5.2.5.3. As vulnerabilidades deverão ser priorizadas considerando, no mínimo:

I. Classificação de criticidade e nível de risco;

II. Probabilidade de exploração e existência de exploits conhecidos;

III. Impacto potencial ao negócio e aos ativos de informação;

IV. Relevância do ativo ou serviço afetado;

V. Prazo esperado para correção.

5.2.5.4. As ações de tratamento deverão ser planejadas, executadas e validadas por responsáveis designados, observando prazos compatíveis com a criticidade da vulnerabilidade e do serviço impactado.

5.2.5.5. As vulnerabilidades deverão ser tratadas de acordo com seu nível de criticidade, observados os prazos e critérios definidos em normas ou procedimentos operacionais complementares.

5.2.5.6. Os testes de validação que apresentarem falhas deverão ser reexecutados até a confirmação da efetiva correção ou mitigação da vulnerabilidade.

5.2.5.7. Caso a correção não seja tecnicamente viável, a situação deverá ser tratada conforme o processo de gestão de exceções e aceite de risco previsto neste Regulamento.

5.2.5.8. Deverão ser estabelecidos mecanismos formais para monitoramento contínuo de vulnerabilidades, incluindo:

I. Acompanhamento de alertas de fabricantes e fornecedores;

II. Utilização de bases especializadas e ferramentas de gestão de vulnerabilidades;

III. Monitoramento de atualizações de segurança e patches disponíveis.

5.2.5.9. Caso uma vulnerabilidade não possa ser corrigida dentro do prazo estabelecido, deverá ser formalizada solicitação de exceção, contendo, no mínimo:

I. Identificação do ativo ou sistema afetado;

II. Descrição detalhada da vulnerabilidade;

III. Avaliação de risco associada;

IV. Justificativa para a não correção no prazo;

V. Controles compensatórios adotados;

VI. Novo prazo para correção;

VII. Plano de ação para remediação.

5.2.5.10. A decisão quanto ao aceite ou não da exceção deverá observar as alçadas de governança definidas.

5.2.5.11. Em caso de aprovação da exceção, a vulnerabilidade deverá permanecer sob monitoramento contínuo até sua efetiva correção.

5.2.6. Gestão de Exceções e Aceite de Risco

5.2.6.1. Quando a correção imediata não for viável por restrições técnicas, operacionais ou contratuais, deverá ser formalizada exceção contendo:

I. Justificativa técnica e impacto;

II. Controles compensatórios adotados;

III. Prazo de reavaliação e/ou correção futura;

IV. Aprovação pela instância competente, conforme a governança de riscos e alçadas internas.

5.2.7. Validação, Reteste e Encerramento

5.2.7.1. A efetividade do tratamento deverá ser verificada por meio de validação e reteste, assegurando que:

I. A vulnerabilidade foi eliminada ou mitigada adequadamente;

II. Não foram introduzidas novas fragilidades relevantes;

III. Os registros e evidências foram arquivados no repositório oficial.

5.2.7.2. O encerramento do registro deverá ocorrer somente após validação, com evidências minimamente suficientes.

5.2.8. Comunicação, Escalonamento e Integração com Incidentes

5.2.8.1. Vulnerabilidades críticas ou de alto risco, especialmente quando houver evidência de exploração ativa, deverão ser escalonadas às instâncias competentes e poderão ensejar:

I. Acionamento do Plano de Resposta a Incidentes;

II. Aplicação de medidas emergenciais;

III. Comunicação a terceiros ou fornecedores responsáveis, quando aplicável;

IV. Acionamento de continuidade, caso haja impacto relevante na operação.

5.2.9. Monitoramento, Indicadores e Melhoria Contínua

5.2.9.1. A Gestão de Vulnerabilidades deverá ser monitorada por indicadores e relatórios periódicos, incluindo, quando aplicável:

I. Volume de vulnerabilidades por criticidade;

II. Tempo médio de tratamento por criticidade;

III. Percentual de conformidade de atualização ou correção;

IV. Reincidência por ativo ou sistema;

V. Exceções e riscos residuais ativos.

5.2.9.2. Os resultados deverão subsidiar a melhoria contínua do SGSI, a atualização de controles e o fortalecimento da postura de segurança da PREVCOM.

5.2.10. Classificação de Vulnerabilidades

5.2.10.1. Para fins de gestão, as vulnerabilidades deverão ser enquadradas, no mínimo, nas seguintes categorias de criticidade:

I. Criticidade Muito Alta: vulnerabilidades com alto potencial de exploração imediata, capazes de comprometer de forma significativa serviços críticos, dados sensíveis ou a continuidade das operações da PREVCOM.

II. Criticidade Alta: vulnerabilidades relevantes, com potencial de exploração e impacto significativo, ainda que parcialmente mitigadas por controles existentes.

III. Criticidade Média: vulnerabilidades com impacto moderado, cuja exploração dependa de condições específicas ou resulte em efeitos limitados aos processos afetados.

IV. Criticidade Baixa: vulnerabilidades com baixo impacto potencial ou cuja exploração seja improvável, não comprometendo significativamente os objetivos institucionais.

5.2.10.2. A classificação de criticidade deverá orientar:

I. A definição de prioridades de tratamento;

II. Os prazos de correção, mitigação ou aceite;

III. A necessidade de escalonamento às instâncias de governança;

IV. A integração com o processo de gestão de riscos e com o Plano de Resposta a Incidentes.

5.2.10.3. Os critérios de avaliação, métricas e prazos de tratamento serão definidos em normas ou procedimentos operacionais complementares.

6. Estrutura e Funções

6.1. Diretoria Executiva

6.1.1. Compete à Diretoria Executiva:

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

II. Deliberar sobre matérias estratégicas relacionadas à gestão de vulnerabilidades;

III. Aplicar as medidas administrativas cabíveis em caso de descumprimento deste Regulamento.

6.2. Diretoria de Tecnologia da Informação

6.2.1. Compete à Diretoria de Tecnologia da Informação:

I. Coordenar, implementar e manter o processo de gestão de vulnerabilidades;

II. Garantir a adoção de ferramentas e controles adequados;

III. Reportar informações relevantes à Diretoria Executiva.

6.3. Equipe de Segurança da Informação

6.3.1. Compete à Equipe de Segurança da Informação:

I. Executar análises de vulnerabilidades;

II. Manter banco de dados de vulnerabilidades identificadas;

III. Acompanhar ações de mitigação, validação e reteste.

6.4. Gestores, Empregados e Prestadores de Serviço

6.4.1. Compete aos gestores, empregados e prestadores de serviço:

I. Cumprir as diretrizes deste Regulamento;

II. Reportar atividades suspeitas ou vulnerabilidades identificadas;

III. Seguir as orientações da Política de Segurança da Informação.

7. Procedimentos

7.1. O processo de gestão de vulnerabilidades técnicas compreende o conjunto de atividades coordenadas destinadas à identificação, análise, tratamento, acompanhamento, verificação e revisão contínua de vulnerabilidades de segurança, com o objetivo de reduzi-las a níveis aceitáveis, em conformidade com as diretrizes do Sistema de Gestão de Segurança da Informação (SGSI) e com as normas ABNT NBR ISO/IEC 27001:2022 e ABNT NBR ISO/IEC 27002:2022.

7.2. Os procedimentos técnicos necessários à execução desse processo, incluindo ferramentas, rotinas específicas, parametrizações, fluxos operacionais, checklists e demais orientações operacionais, serão mantidos em documentos complementares de responsabilidade das áreas competentes.

7.3. Tais documentos deverão:

I. Estar formalmente aprovados pelas instâncias competentes;

II. Ser versionados e controlados;

III. Ser mantidos em repositório oficial da PREVCOM;

IV. Garantir padronização, rastreabilidade e evidências suficientes para auditorias internas e externas;

V. Estar alinhados às diretrizes estabelecidas neste Regulamento e ao SGSI.

7.4. Os procedimentos deverão contemplar, no mínimo, as etapas de mapeamento, monitoramento, tratamento e revisão das vulnerabilidades, assegurando a melhoria contínua dos controles de segurança da informação.

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 revisado 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 90 (noventa) 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 área responsável pela Segurança 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.