PORTARIA Nº. 1.335 DE 29 DE JUNHO DE 2026

LINCOLN DEL BIANCO DE MENEZES CARVALHO, Diretor-Presidente do Bebedouro Previdência – BEBEDOUROPREV, no uso de suas atribuições legais que lhe são conferidas por lei,

RESOLVE

Instituir a Política de Segurança da Informação - PSI do BEBEDOURO PREVIDÊNCIA - BEBEDOUROPREV, e dá outras providências

DA FINALIDADE E FUNDAMENTAÇÃO

Art. 1º Esta Política de Segurança da Informação – PSI tem como finalidade estabelecer as diretrizes corporativas do Bebedouro Previdência - BEBEDOUROPREV para proteção dos ativos de informação e prevenção de responsabilidades legais, devendo ser observada e aplicada por todos os usuários e áreas institucionais.

Art. 2º Esta Política deve ser cumprida integralmente por todos os usuários, servidores, colaboradores, prestadores de serviço e quaisquer terceiros que, direta ou indiretamente, tenham acesso às informações ou recursos tecnológicos do BEBEDOUROPREV.

Art. 3º A PSI está fundamentada nas recomendações da norma ABNT NBR ISO/IEC 27005:2008, reconhecida internacionalmente como código de prática para a gestão da segurança da informação, e observa, ainda, os princípios e obrigações estabelecidos na Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD).

Art. 4º A informação, considerada ativo estratégico de valor para o BEBEDOUROPREV, deve ser adequadamente protegida contra acesso indevido, modificação não autorizada e indisponibilidade indevida, garantindo-se os seguintes princípios:

I – Confidencialidade: garantia de que o acesso à informação seja restrito a pessoas autorizadas;

II – Integridade: garantia de que a informação seja mantida em seu estado original, livre de alterações não autorizadas;

III – Disponibilidade: garantia de que os usuários autorizados tenham acesso às informações sempre que necessário para o desempenho de suas funções.

DOS OBJETIVOS

Art. 5º São objetivos da Política de Segurança da Informação – PSI do BEBEDOUROPREV:

I - Estabelecer princípios, diretrizes e responsabilidades que garantam a proteção das informações institucionais e dos dados pessoais sob a guarda do Instituto, nos termos da legislação vigente e das normas técnicas aplicáveis;

II – Preservar a confidencialidade, integridade e disponibilidade das informações tratadas no âmbito do BEBEDOUROPREV, evitando acessos não autorizados, perdas, alterações indevidas ou interrupções de serviços;

III – Garantir a conformidade com a Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD), especialmente no que tange ao tratamento lícito, transparente e seguro de dados pessoais de segurados, servidores, fornecedores e demais titulares;

IV – Prevenir incidentes de segurança da informação e mitigar riscos operacionais e reputacionais por meio da implementação de controles técnicos e administrativos adequados;

V – Estabelecer padrões e normas para o uso adequado dos recursos tecnológicos e informacionais do BEBEDOUROPREV, promovendo a responsabilidade digital entre os usuários;

VI – Promover a cultura organizacional de segurança da informação, mediante ações de sensibilização, capacitação e comunicação contínuas;

VII – Assegurar a rastreabilidade e auditabilidade dos acessos e operações realizadas em ambientes informatizados e processos críticos da organização;

VIII – Servir de base para a elaboração de normas complementares, planos de contingência, procedimentos operacionais e demais documentos relacionados à segurança da informação e à proteção de dados pessoais.

DAS APLICAÇÕES E CONFORMIDADE

Art. 6º Esta Política aplica-se a todos os servidores, colaboradores, estagiários, fornecedores, prestadores de serviços e quaisquer terceiros que, de forma direta ou indireta, tenham acesso a informações, sistemas, dados pessoais ou recursos tecnológicos no âmbito do BEBEDOUROPREV.

Art. 7º O disposto nesta Política está em conformidade com a Lei Federal nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD), e será observado em todos os processos que envolvam o tratamento de dados pessoais no Instituto, inclusive nos ambientes físicos e digitais.

§1º O tratamento de dados pessoais, em qualquer fase (coleta, armazenamento, uso, compartilhamento ou eliminação), deverá respeitar os seguintes princípios:

I – Finalidade: os dados devem ser tratados para propósitos legítimos, específicos e informados ao titular;

II – Adequação: o tratamento deve ser compatível com a finalidade informada;

III – Necessidade: limitação do tratamento ao mínimo necessário;

IV – Livre acesso: garantia de consulta facilitada pelo titular sobre o tratamento de seus dados;

V – Qualidade dos dados: exatidão, clareza, relevância e atualização dos dados;

VI – Transparência: informação clara aos titulares, resguardados os segredos comercial e institucional;

VII – Segurança: uso de medidas técnicas e administrativas para proteção contra acessos não autorizados e danos;

VIII – Prevenção: adoção de medidas para evitar a ocorrência de danos;

IX – Não discriminação: tratamento dos dados sem fins discriminatórios ou abusivos;

X – Responsabilização e prestação de contas: demonstração da adoção de medidas eficazes para o cumprimento da LGPD.

Art. 8º Todos os envolvidos na execução de atividades institucionais, incluindo os que realizarem o tratamento de dados pessoais, deverão firmar Termo de Responsabilidade, comprometendo-se a cumprir integralmente esta Política e os normativos complementares.

DAS RESPONSABILIDADES

Art. 9º. São responsáveis pela aplicação e observância desta Política:

I – Os servidores públicos efetivos ou comissionados vinculados ao BEBEDOUROPREV;

II – Os estagiários, colaboradores e prestadores de serviços contratados;

III – Os Diretores;

IV – A Comissão de Segurança da Informação;

V – Os fornecedores e terceiros com acesso às informações.

§1º Compete aos usuários em geral:

a) Manter sigilo e confidencialidade sobre todas as informações acessadas no exercício de suas funções;

b) Utilizar os recursos tecnológicos do BEBEDOUROPREV apenas para fins institucionais;

c) Observar e cumprir as diretrizes estabelecidas nesta Política e em seus normativos complementares;

d) Zelar pela guarda de senhas, tokens, dispositivos de autenticação e quaisquer mecanismos de segurança que lhes forem atribuídos;

e) Comunicar imediatamente quaisquer incidentes de segurança ou suspeitas de violação de dados à área responsável.

§2º Compete aos diretores:

a) Assegurar que todos os membros da sua equipe conheçam e cumpram esta Política;

b) Estimular a cultura de segurança da informação em sua área de atuação;

c) Reportar situações de risco ou de descumprimento à área de Segurança da Informação;

d) Garantir que, ao desligamento ou realocação de servidores e colaboradores, os acessos sejam devidamente revogados.

§3º Compete à Comissão de Segurança da Informação:

a) Implementar, manter e revisar os controles técnicos de segurança da informação;

b) Garantir a disponibilidade, integridade e confidencialidade dos sistemas e dados institucionais;

c) Realizar auditorias e monitoramento de acessos e eventos de segurança;

d) Atuar em conjunto com a Comissão de Segurança da Informação para a análise e tratamento de incidentes.

f) Estabelecer diretrizes estratégicas para a aplicação e revisão da PSI;

g) Avaliar riscos e propor medidas de mitigação;

h) Acompanhar auditorias e propor planos de ação corretiva;

i) Estimular a disseminação da cultura de segurança da informação.

§4º Compete aos fornecedores e terceiros:

a) Cumprir as obrigações contratuais relacionadas à proteção de dados e segurança da informação;

b) Utilizar as informações institucionais apenas para as finalidades previstas em contrato;

c) Observar integralmente a LGPD e os demais normativos aplicáveis;

d) Assinar termo de compromisso e confidencialidade antes de acessar quaisquer dados ou sistemas do BEBEDOUROPREV.

Parágrafo único. O descumprimento das responsabilidades definidas neste artigo poderá acarretar sanções administrativas, civis e/ou penais, conforme a gravidade da infração e a legislação vigente.

DO CONTROLE DE ACESSO

Art. 10. O controle de acesso às informações e aos sistemas do BEBEDOUROPREV será realizado com base nos princípios da confidencialidade, integridade, disponibilidade e mínima concessão de privilégios.

§1º Todo usuário deverá possuir credenciais de acesso individuais, intransferíveis e protegidas por senha forte.

§2º Os acessos serão concedidos conforme a função, atribuição e necessidade do usuário, sendo periodicamente revistos pela área de Tecnologia da Informação.

§3º A criação, alteração ou revogação de acessos dependerá de solicitação formal e autorização do gestor da área demandante.

§4º É vedado o compartilhamento de senhas, logins ou outros dispositivos de autenticação.

§5º O acesso físico a ambientes sensíveis será restrito a pessoas autorizadas, mediante mecanismos de autenticação física ou registros de entrada.

§6º Todos os acessos lógicos e físicos relevantes deverão ser registrados e armazenados por prazo mínimo previsto em norma complementar, com vistas à auditoria e à responsabilização.

Art. 11. No caso de desligamento, exoneração, realocação ou substituição de usuários, os acessos deverão ser imediatamente revogados ou ajustados pela área de TI, mediante aviso da unidade gestora responsável.

Parágrafo único. A inobservância dos procedimentos de controle de acesso constitui infração sujeita às penalidades previstas nesta Política.

DO USO DE DISPOSITIVOS MÓVEIS

Art. 12. O uso de dispositivos móveis no âmbito do BEBEDOUROPREV deverá observar rigorosamente os princípios da segurança da informação e da proteção de dados pessoais, conforme estabelecido na Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD).

§1º Consideram-se dispositivos móveis os notebooks, tablets, smartphones, pendrives e quaisquer equipamentos eletrônicos portáteis com capacidade de armazenamento, transmissão ou tratamento de informações.

§2º O uso de dispositivos móveis de propriedade do BEBEDOUROPREV, ou de terceiros autorizados, será condicionado à aprovação da área de Tecnologia da Informação e à formalização de termo de responsabilidade.

§3º Os dispositivos móveis utilizados em atividades institucionais deverão conter, obrigatoriamente:

I - autenticação por senha forte ou biometria;

II - antivírus atualizado;

III - criptografia de dados;

IV - bloqueio automático por inatividade;

V - restrições de instalação de aplicativos não autorizados.

§4º É vedada a instalação de softwares ou aplicações sem prévia anuência da Comissão de Segurança de Informação, bem como qualquer alteração na configuração original de segurança.

§5º Em caso de extravio, furto, roubo ou qualquer incidente de segurança que envolva dispositivo móvel institucional, o usuário deverá comunicar imediatamente à chefia imediata e

à Comissão de Segurança de Informação, a fim de viabilizar a mitigação dos riscos e a adoção de providências legais e administrativas.

§6º Os dados pessoais eventualmente armazenados em dispositivos móveis deverão ser protegidos contra acesso indevido, respeitando-se os princípios da minimização, finalidade e necessidade, nos termos da LGPD.

§7º É responsabilidade do usuário garantir a guarda, o uso adequado e a devolução do equipamento ao final do vínculo funcional ou em caso de substituição.

§8º A violação das regras aqui estabelecidas poderá ensejar responsabilização do servidor ou prestador de serviço, conforme previsto nesta Política e na legislação vigente.

DOS PROCEDIMENTOS DE BACKUP

Art. 13. O BEBEDOUROPREV deverá manter procedimentos de backup que garantam a integridade, disponibilidade e recuperação tempestiva dos dados e sistemas informatizados, em conformidade com os princípios da segurança da informação e com as exigências da Lei Geral de Proteção de Dados Pessoais – LGPD.

§1º Os backups deverão ser realizados de forma automatizada, com periodicidade definida por política interna, preferencialmente fora do horário comercial.

§2º As cópias de segurança deverão ser armazenadas em locais seguros, com proteção contra incêndio, umidade, acesso não autorizado e falhas de equipamento, inclusive em ambientes distintos do local de produção dos dados.

§3º Os procedimentos de backup deverão prever:

I – a integridade e o versionamento dos dados copiados;

II – a identificação clara das mídias e arquivos gerados;

III – a guarda em local com controle de acesso físico, conforme normas técnicas da ABNT;

IV – a realização de testes periódicos de restauração (restore), com registros documentais dos resultados;

V – a confidencialidade dos dados pessoais eventualmente incluídos nos backups, com mecanismos de criptografia e acesso restrito.

§4º A área de Tecnologia da Informação será responsável por:

I – manter inventário atualizado das mídias e registros de backup;

II – definir e aplicar os prazos de retenção conforme o grau de criticidade da informação e a legislação vigente;

III – promover a substituição periódica das mídias de armazenamento, conforme recomendações técnicas;

IV – controlar os acessos às cópias de segurança e assegurar a rastreabilidade.

§5º Em caso de falha no processo de backup ou de restauração, o responsável técnico deverá realizar nova execução assim que sanado o problema, priorizando os sistemas críticos e comunicando o incidente à autoridade competente.

§6º A inobservância das normas de backup configura infração grave à Política de Segurança da Informação e poderá acarretar responsabilização administrativa, civil e/ou penal do agente envolvido.

DA PRIVACIDADE DA INFORMAÇÃO

Art. 14. O BEBEDOUROPREV assegura o respeito à privacidade dos dados pessoais e sensíveis sob sua guarda, em conformidade com a Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD).

§1º A coleta, o tratamento, o armazenamento e o compartilhamento de dados pessoais devem observar:

I - a finalidade específica e legítima;

II - a necessidade mínima dos dados para atingir a finalidade proposta;

III - o livre acesso dos titulares às informações que lhes digam respeito;

IV - a qualidade e exatidão dos dados armazenados;

V - a transparência no tratamento de dados, respeitados os segredos institucionais e comerciais;

VI - a segurança dos dados contra acessos não autorizados e situações acidentais ou ilícitas.

§2º O acesso às informações e dados pessoais será restrito a pessoas devidamente autorizadas e capacitadas, com registro formal de autorização.

§3º Toda informação tratada no âmbito do BEBEDOUROPREV é considerada patrimônio institucional e deverá ser protegida, inclusive após o término do vínculo do servidor ou colaborador com a autarquia.

§4º O compartilhamento de dados pessoais com terceiros exige autorização do Diretor-Presidente ou base legal definida pela LGPD, devendo ser precedido de avaliação de risco e celebração de instrumentos contratuais com cláusulas específicas de proteção de dados.

DO MONITORAMENTO E DA AUDITORIA

Art. 15. O BEBEDOUROPREV poderá adotar mecanismos de monitoramento e auditoria em seus ambientes físicos e digitais, com o objetivo de garantir o cumprimento desta Política, assegurar a integridade dos ativos de informação, prevenir incidentes de segurança e promover a responsabilização de agentes infratores.

§1º Os acessos a redes, sistemas, e-mails, aplicativos, dispositivos móveis, recursos em nuvem e demais infraestruturas tecnológicas poderão ser monitoradas, registrados e auditados com base em critérios técnicos previamente definidos pela Comissão de Segurança da Informação.

§2º O monitoramento deverá observar rigorosamente os princípios da legalidade, proporcionalidade, necessidade, finalidade e transparência, garantindo-se o respeito à privacidade individual e à proteção de dados pessoais, conforme a Lei nº 13.709/2018 – LGPD.

§3º A auditoria técnica de sistemas, equipamentos, ambientes, acessos e processos poderá ser realizada:

I - periodicamente, conforme plano anual de auditoria de segurança da informação;

II - extraordinariamente, em caso de incidentes, falhas, denúncias ou suspeitas de violação de segurança;

III - por demanda da Controladoria Interna, da Comissão de Segurança da Informação ou do Diretor-Presidente;

IV - por exigência de órgãos de controle, fiscalização ou auditoria externa.

§4º Os relatórios de auditoria e os logs de acesso deverão ser armazenados em ambiente seguro, com controle de integridade e acesso restrito, respeitando os prazos legais e os critérios definidos na política de classificação e temporalidade da informação.

§5º As evidências de uso indevido, falhas, condutas inadequadas ou violações de segurança identificadas em auditorias deverão ser formalmente registradas e encaminhadas às instâncias competentes, podendo ensejar abertura de processo administrativo disciplinar, comunicação à autoridade de proteção de dados ou à autoridade policial, conforme a gravidade do caso.

§6º A critério da Comissão de Segurança da Informação, poderão ser utilizados sistemas de correlação de eventos, inteligência artificial ou soluções automatizadas de análise comportamental e detecção de anomalias, desde que observadas as salvaguardas legais de proteção à privacidade.

Parágrafo único. As atividades de monitoramento e auditoria deverão ser detalhadas em norma interna complementar e serão realizadas com base em plano formal, auditável, com registros rastreáveis, preservando-se o equilíbrio entre o controle institucional e os direitos fundamentais do usuário. As atividades de monitoramento e auditoria serão regulamentadas em instrumento normativo complementar, garantindo-se o equilíbrio entre o controle institucional e os direitos individuais.

DAS COMPETÊNCIAS DO RESPONSÁVEL PELA GESTÃO DE SEGURANÇA DA INFORMAÇÃO

Art. 16. A Comissão de Segurança da Informação será responsável pela gestão da segurança da informação, que atuará como ponto focal para as ações de proteção dos ativos informacionais e de conformidade com esta Política.

§1º Compete ao responsável pela gestão da segurança da informação:

a) prover todas as informações relativas à Gestão de Segurança da Informação no âmbito da unidade gestora do BEBEDOUROPREV;

b) garantir a ampla divulgação desta Política e das normas complementares para todos os servidores e prestadores de serviços;

c) promover ações contínuas de conscientização sobre segurança da informação, incluindo treinamentos, campanhas e orientações operacionais;

d) propor projetos, medidas técnicas e organizacionais para o aperfeiçoamento da segurança da informação;

e) elaborar e manter atualizada a política de classificação da informação, incluindo a definição de temporalidade de guarda documental;

f) apoiar as ações de classificação e organização documental no caso de inexistência de Arquivo Público estruturado, podendo, para isso, contar com o suporte de servidor específico do ente federativo ou do BEBEDOUROPREV.

§2º O responsável pela gestão da segurança da informação atuará em colaboração com a Comissão de Segurança da Informação e com as demais áreas estratégicas do Instituto, reportando periodicamente suas ações ao Diretor-Presidente.

DA COMISSÃO DE SEGURANÇA DA INFORMAÇÃO

Art. 17. Fica instituída, no âmbito do BEBEDOUROPREV, a Comissão de Segurança da Informação, com a finalidade de definir, apoiar e acompanhar a implementação, manutenção e constante aprimoramento da Política de Segurança da Informação – PSI.

§1º A Comissão será composta, no mínimo, pelos seguintes membros:

a) o(a) Diretor de Administração Geral, Gestão de Pessoal e Previdência;

b) o(a) Controlador(a) Interno(a);

c) o(a) Ouvidor Previdenciário.

§2º Compete à Comissão de Segurança da Informação:

I - propor e validar as estratégias e ações necessárias para garantir a aplicação da PSI em todas as unidades e processos;

II - promover a revisão periódica da Política de Segurança da Informação, no mínimo a cada 4 (quatro) anos ou sempre que houver mudanças significativas na estrutura tecnológica, regulatória ou organizacional do BEBEDOUROPREV;

III - estabelecer critérios e procedimentos para auditorias internas de segurança da informação e rastreabilidade de acessos a sistemas críticos;

IV - aprovar e acompanhar os planos de contingência, continuidade de negócios e recuperação de desastres no âmbito da gestão da informação;

V - apoiar a difusão da cultura de segurança da informação entre os servidores e colaboradores, por meio de treinamentos e campanhas educativas;

VI - deliberar sobre incidentes de segurança classificados como críticos, definindo medidas corretivas e preventivas a serem adotadas.

§3º As reuniões da Comissão ocorrerão de forma ordinária semestralmente e, de forma extraordinária, sempre que convocadas por qualquer de seus membros.

§4º As deliberações da Comissão deverão ser registradas em ata formal e arquivadas de forma segura e acessível para fins de auditoria e governança.

DAS INFRAÇÕES E PENALIDADES

Art. 18. O descumprimento das disposições desta Política sujeitará os responsáveis às sanções previstas em normativos internos, na legislação administrativa aplicável e, especialmente, na Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD), observados os princípios do contraditório e da ampla defesa.

§1º As infrações serão analisadas considerando sua natureza, gravidade, impacto institucional, prejuízos a titulares de dados e reincidência, podendo ser classificadas como:

I - Leves: condutas que contrariem diretrizes da PSI sem prejuízos identificáveis;

II - Médias: ações ou omissões que comprometam a segurança da informação de forma moderada;

III - Graves: condutas dolosas ou que resultem em prejuízo à integridade, confidencialidade ou disponibilidade de dados institucionais ou pessoais, ou que caracterizem violação à LGPD.

§2º As penalidades aplicáveis incluem, conforme o caso:

I - Advertência verbal ou escrita;

II - Suspensão de acesso a sistemas e recursos informacionais;

III - Responsabilização funcional, contratual, civil e/ou penal;

IV - Demissão por justa causa, nos casos previstos em lei;

V - Indenização por danos causados a terceiros ou à instituição, nos termos da legislação vigente.

§3º Nos casos em que a violação da Política envolver tratamento indevido de dados pessoais, serão aplicáveis também as sanções previstas nos arts. 52 a 54 da LGPD, incluindo:

I - advertência, com indicação de prazo para adoção de medidas corretivas;

II - bloqueio ou eliminação dos dados pessoais envolvidos, quando aplicável;

III - comunicação aos titulares dos dados afetados;

IV - outras medidas recomendadas pela legislação vigente.

§4º O Diretor-Presidente, mediante parecer da Comissão de Segurança da Informação, decidirá sobre a penalidade a ser aplicada, podendo também encaminhar o caso às autoridades competentes.

DAS DISPOSIÇÕES FINAIS

Art. 19. A presente Política de Segurança da Informação deverá ser amplamente divulgada, publicada no sítio eletrônico oficial do BEBEDOUROPREV e incorporada aos processos de integração de novos servidores e colaboradores.

Art. 20. A Política de Segurança da Informação deverá ser revista periodicamente, no máximo a cada 4 (quatro) anos, ou sempre que houver mudanças relevantes na legislação, nos processos institucionais ou nos sistemas de informação utilizados.

Art. 21. Os casos omissos ou situações não previstas nesta Política serão analisados pela Comissão de Segurança da Informação, com parecer técnico da área de Tecnologia da Informação, e submetidos à decisão do Diretor-Presidente.

Art. 22. Esta Política entra em vigor na data de sua aprovação e revoga disposições anteriores que lhe sejam contrárias.

Cientifique-se, publique-se e cumpra-se.
Bebedouro, 30 de junho de 2026.

Lincoln Del Bianco de Menezes Carvalho
Diretor-Presidente do BEBEDOUROPREV –
Registrada e publicada a presente Portaria na imprensa oficial, em 30 de junho de 2026.

TERMO DE CIÊNCIA E CONHECIMENTO DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DO BEBEDOURO PREVIDÊNCIA - BEBEDOUROPREV

Declaro que recebi a Política de Segurança da Informação - PSI do BEBEDOURO PREVIDÊNCIA - BEBEDOUROPREV, estando ciente de seu conteúdo e da sua importância para o bom exercício funcional do próprio BEBEDOURO PREVIDÊNCIA - BEBEDOUROPREV.

A assinatura do presente Termo, anexo a referida Política de Segurança da Informação, é manifestação de minha concordância e do meu compromisso em cumpri-lo integralmente.

Bebedouro/SP, XX de XXXXX de 20XX.

_____

NOME COMPLETO
(CARGO)