POLÍTICA COMPLEMENTAR DE SEGURANÇA DA INFORMAÇÃO – PSI

Atualiza a Política Complementar de Segurança da Informação – PSI da Subsecretaria de Gestão Previdenciária – SUPREV e estabelece diretrizes para a proteção das informações e dos ativos de informação sob sua responsabilidade.

1. OBJETIVO

A Política Complementar de Segurança da Informação – PSI estabelece princípios, diretrizes e responsabilidades para a proteção das informações e dos ativos de informação utilizados pela Subsecretaria de Gestão Previdenciária – SUPREV.

A Política tem por objetivo preservar a **confidencialidade, integridade, disponibilidade, autenticidade e rastreabilidade** das informações, bem como assegurar o adequado tratamento dos dados pessoais e a continuidade dos serviços, contribuindo para a redução dos riscos de segurança da informação e para a proteção dos interesses institucionais da SUPREV.

São também objetivos desta Política:

I – orientar os usuários quanto à utilização segura das informações, sistemas, equipamentos e demais recursos tecnológicos;

II – estabelecer responsabilidades relacionadas à segurança da informação;

III – prevenir, identificar, comunicar e tratar incidentes de segurança da informação;

IV – estabelecer diretrizes para proteção dos dados pessoais e das informações institucionais;

V – promover a cultura de segurança da informação por meio de capacitação e conscientização;

VI – estabelecer diretrizes para gestão de riscos relacionados à segurança da informação;

VII – contribuir para a continuidade e a recuperação dos serviços e informações essenciais da SUPREV.

2. FUNDAMENTAÇÃO

Esta Política observa, no que couber:

I – a legislação federal e municipal aplicável à segurança da informação e à proteção de dados pessoais;

II – a Lei Federal nº 12.527, de 18 de novembro de 2011 – Lei de Acesso à Informação;

III – a Lei Federal nº 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais – LGPD;

IV – o Decreto Municipal nº 15.423, de 19 de dezembro de 2013, que institui a Política de Segurança da Informação no âmbito da Administração Direta e Indireta do Poder Executivo Municipal;

V – o Decreto Municipal nº 18.608, de 18 de janeiro de 2024, que regulamenta a Lei Geral de Proteção de Dados Pessoais no âmbito da Administração Direta e Indireta do Poder Executivo;

VI – as normas, políticas, instruções normativas, padrões e procedimentos estabelecidos pela Prefeitura de Belo Horizonte e pela PRODABEL;

VII – as normas técnicas aplicáveis, especialmente a ABNT NBR ISO/IEC 27001 e a ABNT NBR ISO/IEC 27002, em suas versões vigentes.

Na hipótese de conflito entre esta Política e norma superior, prevalecerá a norma hierarquicamente superior.

3. ABRANGÊNCIA

Esta Política aplica-se a todos os servidores, ocupantes de cargos em comissão, empregados, contratados, estagiários, prestadores de serviços, fornecedores e demais pessoas que, em razão de suas atividades, tenham acesso às informações, sistemas, equipamentos, redes ou demais ativos de informação da SUPREV.

Aplica-se às informações produzidas, recebidas, armazenadas, processadas ou transmitidas pela SUPREV, independentemente do meio ou suporte utilizado, incluindo ambientes físicos, digitais, sistemas corporativos, dispositivos móveis, serviços de computação em nuvem e demais recursos tecnológicos institucionais.

4. PRINCÍPIOS DA SEGURANÇA DA INFORMAÇÃO

A segurança da informação na SUPREV observará, entre outros, os seguintes princípios:

4.1. Confidencialidade

As informações deverão ser acessadas somente por pessoas autorizadas e na medida necessária ao desempenho de suas atribuições.

4.2. Integridade

As informações deverão ser protegidas contra alterações, exclusões ou modificações indevidas, intencionais ou acidentais.

4.3. Disponibilidade

As informações e os serviços essenciais deverão estar disponíveis aos usuários autorizados sempre que necessários ao desempenho das atividades institucionais.

4.4. Autenticidade

Deverá ser assegurada a identificação adequada da origem das informações, dos usuários e das operações realizadas nos sistemas institucionais.

4.5. Rastreabilidade

As ações relevantes realizadas sobre sistemas, informações e recursos tecnológicos deverão ser passíveis de identificação e auditoria, observadas as normas aplicáveis.

4.6. Privacidade e proteção de dados pessoais

O tratamento de dados pessoais deverá observar a legislação aplicável, os princípios da proteção de dados e as orientações institucionais da Prefeitura de Belo Horizonte.

4.7. Gestão baseada em riscos

As medidas de segurança deverão considerar a natureza, a criticidade, o valor e os riscos associados às informações, sistemas, processos e serviços.

4.8. Responsabilidade

Cada usuário é responsável pelo uso adequado das informações, sistemas e recursos que lhe forem disponibilizados, de acordo com suas atribuições e níveis de acesso.

5. DIRETRIZES GERAIS

A informação constitui ativo estratégico para a SUPREV e deverá ser protegida durante todo o seu ciclo de vida, desde sua criação ou recebimento até seu armazenamento, utilização, compartilhamento, arquivamento e descarte.

As informações institucionais deverão ser utilizadas exclusivamente para finalidades relacionadas às atividades da Administração Pública, ressalvadas as situações expressamente autorizadas.

O acesso às informações e aos recursos tecnológicos deverá observar os princípios da necessidade de conhecimento e do menor privilégio, sendo concedido somente na extensão necessária ao desempenho das atribuições do usuário.

Os recursos tecnológicos institucionais deverão ser utilizados de forma responsável, segura e compatível com as normas da Prefeitura de Belo Horizonte e da PRODABEL.

É vedada a utilização dos recursos institucionais para atividades que comprometam a segurança, a disponibilidade, a integridade ou a imagem institucional da SUPREV ou da Prefeitura de Belo Horizonte.

6. CLASSIFICAÇÃO E TRATAMENTO DAS INFORMAÇÕES

As informações deverão receber tratamento compatível com seu grau de sensibilidade, criticidade e restrição de acesso, observada a legislação aplicável.

As informações que contenham dados pessoais, dados pessoais sensíveis, informações sigilosas ou informações estratégicas deverão receber proteção compatível com os riscos associados.

O compartilhamento de informações deverá ocorrer somente com pessoas ou instituições legitimamente autorizadas e para finalidades institucionais definidas.

A reprodução, impressão, cópia, transferência, armazenamento ou descarte de informações deverá observar os controles de segurança aplicáveis.

Documentos físicos que contenham informações protegidas deverão permanecer em locais adequados e com acesso restrito às pessoas autorizadas.

7. CONTROLE DE ACESSO

Os acessos aos sistemas, aplicações, equipamentos e demais recursos tecnológicos deverão ser individualizados e vinculados a uma pessoa específica, sempre que tecnicamente possível.

É proibido compartilhar senhas, credenciais, certificados digitais ou outros mecanismos de autenticação individual.

A concessão de acesso deverá observar autorização formal e os princípios da necessidade de conhecimento e do menor privilégio.

Os acessos deverão ser alterados ou revogados quando houver mudança de função, afastamento, desligamento ou quando deixarem de ser necessários.

Os acessos privilegiados ou administrativos deverão receber controles adicionais, conforme os padrões estabelecidos pela área competente de tecnologia da informação.

O usuário é responsável pela proteção de suas credenciais e deverá comunicar imediatamente qualquer suspeita de uso indevido ou comprometimento de suas credenciais.

8. USO DE RECURSOS TECNOLÓGICOS

Computadores, sistemas, redes, dispositivos móveis, serviços de armazenamento, correio eletrônico e demais recursos tecnológicos disponibilizados pela Administração deverão ser utilizados de forma segura e compatível com as atividades institucionais.

É vedada a instalação de softwares, aplicativos ou recursos tecnológicos não autorizados nos equipamentos institucionais, quando houver possibilidade de comprometimento da segurança do ambiente.

O armazenamento de informações institucionais deverá ocorrer, preferencialmente, em ambientes corporativos oficialmente disponibilizados e submetidos aos mecanismos institucionais de segurança, controle de acesso, backup e recuperação.

O uso pessoal eventual dos recursos institucionais somente será admitido quando permitido pelas normas vigentes e desde que não comprometa a segurança, o desempenho ou a finalidade institucional dos recursos.

9. USO DE INTELIGÊNCIA ARTIFICIAL

A utilização de ferramentas de Inteligência Artificial – IA no âmbito da SUPREV deverá observar os princípios de segurança da informação, proteção de dados pessoais, confidencialidade, integridade, transparência e responsabilidade.

É vedada a inserção, em ferramentas de IA não autorizadas ou não homologadas institucionalmente, de informações sigilosas, dados pessoais, dados pessoais sensíveis, credenciais de acesso ou informações estratégicas da Administração.

Somente poderão ser utilizadas, para fins institucionais, ferramentas de IA autorizadas pelos órgãos competentes da Prefeitura de Belo Horizonte, observadas as orientações e listas atualizadas de ferramentas permitidas.

Conteúdos produzidos ou apoiados por IA deverão ser submetidos à revisão e validação humana antes de sua utilização, divulgação, publicação ou incorporação a processos administrativos ou decisões institucionais.

O usuário será responsável pela verificação da exatidão, pertinência, segurança, legalidade e adequação das informações produzidas ou processadas com auxílio de ferramentas de IA.

A utilização de IA não exime o agente público de sua responsabilidade pela decisão, manifestação ou documento produzido.

10. DISPOSITIVOS MÓVEIS E ACESSO REMOTO

Os dispositivos móveis utilizados para acesso a informações ou recursos institucionais deverão observar os requisitos de segurança definidos pela Prefeitura de Belo Horizonte e pela PRODABEL.

O usuário deverá adotar medidas para impedir o acesso não autorizado ao equipamento, inclusive mediante utilização de mecanismos de autenticação e bloqueio.

A perda, furto, roubo ou comprometimento de dispositivo utilizado para acesso a informações institucionais deverá ser comunicado imediatamente aos canais institucionais competentes.

O acesso remoto aos ambientes institucionais deverá utilizar mecanismos autorizados e seguros.

11. SEGURANÇA DE FORNECEDORES E TERCEIROS

Fornecedores, prestadores de serviços e demais terceiros que tenham acesso a informações ou recursos tecnológicos da SUPREV deverão observar as normas de segurança da informação aplicáveis.

Os contratos e instrumentos equivalentes deverão prever, quando cabível, obrigações relacionadas à confidencialidade, proteção de dados, segurança da informação, controle de acesso, comunicação de incidentes e devolução ou eliminação das informações ao término da relação contratual.

O acesso de terceiros deverá ser limitado ao estritamente necessário para a execução das atividades contratadas e deverá ser revogado quando deixar de ser necessário.

12. GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

Todo usuário deverá comunicar imediatamente qualquer incidente ou suspeita de incidente de segurança da informação aos canais institucionais definidos pela SUPREV ou pela PRODABEL.

São exemplos de incidentes ou situações que deverão ser comunicados:

I – acesso não autorizado a sistemas ou informações;

II – perda, furto ou roubo de equipamento;

III – divulgação ou envio indevido de informações;

IV – suspeita de vazamento de dados pessoais;

V – recebimento de mensagens ou arquivos suspeitos;

VI – comprometimento ou suspeita de comprometimento de credenciais;

VII – alteração ou exclusão indevida de informações;

VIII – indisponibilidade inesperada de sistemas ou serviços;

IX – identificação de malware ou comportamento anormal de equipamentos;

X – qualquer outra situação que possa comprometer a confidencialidade, integridade ou disponibilidade das informações.

O usuário não deverá ocultar, apagar ou alterar evidências relacionadas a eventual incidente, salvo orientação da área responsável pelo tratamento do incidente.

O tratamento dos incidentes deverá observar os procedimentos e fluxos estabelecidos pela Prefeitura de Belo Horizonte e pela PRODABEL.

13. BACKUP, CONTINUIDADE E RECUPERAÇÃO

As informações e sistemas considerados relevantes ou críticos deverão estar submetidos aos mecanismos institucionais de backup, continuidade e recuperação definidos pela Prefeitura de Belo Horizonte e pela PRODABEL.

Os usuários deverão armazenar os arquivos institucionais nos ambientes corporativos disponibilizados para essa finalidade, observando as orientações de segurança e armazenamento.

Deverão ser adotadas medidas destinadas a reduzir os riscos de perda, indisponibilidade ou comprometimento das informações e serviços essenciais.

Os procedimentos técnicos de realização, armazenamento, retenção e recuperação de cópias de segurança serão estabelecidos em instrumentos específicos.

14. MONITORAMENTO, REGISTROS E AUDITORIA

Os ambientes, sistemas, redes e equipamentos institucionais poderão ser monitorados, registrados e auditados, nos limites estabelecidos pela legislação e pelas normas aplicáveis, para fins de segurança, prevenção de incidentes, investigação, continuidade dos serviços e proteção dos ativos institucionais.

Os registros de acesso e eventos de segurança deverão ser mantidos e protegidos conforme os requisitos técnicos e legais aplicáveis.

O monitoramento deverá observar os princípios de necessidade, finalidade, proporcionalidade, segurança e proteção de dados pessoais.

15. SEGURANÇA DAS INFORMAÇÕES EM MEIO FÍSICO

Informações físicas que contenham dados pessoais, informações sigilosas ou outros conteúdos protegidos deverão ser armazenadas em locais seguros e com acesso restrito.

A retirada, consulta, movimentação, reprodução ou descarte de documentos físicos deverá observar os procedimentos institucionais aplicáveis.

É vedada a retirada de documentos ou informações físicas das dependências institucionais sem autorização, quando houver restrição decorrente de sua natureza ou classificação.

Documentos que contenham informações protegidas deverão ser descartados de forma segura, de modo a impedir sua recuperação ou utilização indevida.

16. PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS

O tratamento de dados pessoais realizado no âmbito da SUPREV deverá observar a Lei Federal nº 13.709/2018 – LGPD, o Decreto Municipal nº 18.608/2024 e demais normas e orientações aplicáveis.

Os dados pessoais deverão ser:

I – coletados e tratados para finalidades legítimas e institucionais;

II – acessados somente por pessoas autorizadas e na medida necessária ao exercício de suas atribuições;

III – protegidos contra acesso não autorizado, perda, alteração, destruição ou divulgação indevida;

IV – compartilhados somente quando houver fundamento legal e observância dos requisitos aplicáveis;

V – armazenados e eliminados de acordo com as regras de retenção e gestão documental aplicáveis.

O tratamento de dados pessoais sensíveis deverá observar controles de segurança compatíveis com sua natureza e os riscos envolvidos.

Situações que possam caracterizar incidente envolvendo dados pessoais deverão ser comunicadas imediatamente aos canais institucionais competentes.

17. RESPONSABILIDADES

17.1. Dos usuários

Compete aos usuários:

I – cumprir esta Política e as normas complementares de segurança da informação;

II – proteger suas credenciais e os recursos tecnológicos sob sua responsabilidade;

III – utilizar as informações somente para finalidades autorizadas;

IV – comunicar incidentes ou suspeitas de incidentes;

V – participar das ações de capacitação e conscientização promovidas pela Administração;

VI – preservar a confidencialidade das informações a que tenham acesso em razão de suas atividades, inclusive após o encerramento do vínculo, quando aplicável.

17.2. Dos gestores

Compete aos gestores:

I – promover o cumprimento desta Política em suas unidades;

II – assegurar que os acessos concedidos aos usuários sejam compatíveis com suas atribuições;

III – comunicar alterações de função, afastamentos e desligamentos que impliquem alteração ou revogação de acessos;

IV – orientar suas equipes quanto às responsabilidades relacionadas à segurança da informação;

V – apoiar a participação dos servidores nas ações de capacitação e conscientização.

17.3. Da área responsável pela Tecnologia da Informação

Compete à área responsável pela Tecnologia da Informação:

I – apoiar a implementação dos controles de segurança da informação;

II – orientar os usuários quanto à utilização segura dos recursos tecnológicos;

III – apoiar a identificação e o tratamento de incidentes;

IV – acompanhar os riscos tecnológicos relacionados aos ambientes sob sua responsabilidade;

V – promover ou apoiar ações de monitoramento, prevenção e melhoria da segurança dos recursos tecnológicos;

VI – observar e fazer cumprir as normas e padrões técnicos estabelecidos pela Prefeitura de Belo Horizonte e pela PRODABEL.

17.4. Da gestão da SUPREV

Compete à SUPREV:

I – promover a implementação e o cumprimento desta Política;

II – estabelecer responsabilidades e mecanismos de governança de segurança da informação;

III – promover ações de capacitação e conscientização;

IV – acompanhar riscos e incidentes relevantes;

V – promover a revisão e o aprimoramento contínuo desta Política.

18. CAPACITAÇÃO E CONSCIENTIZAÇÃO

Deverão ser promovidas ações periódicas de capacitação e conscientização em segurança da informação, considerando os riscos associados às atividades desenvolvidas.

As ações deverão abordar, quando aplicável:

I – proteção de credenciais;

II – prevenção contra phishing e engenharia social;

III – proteção de dados pessoais;

IV – uso adequado dos recursos tecnológicos;

V – comunicação de incidentes;

VI – uso seguro de ferramentas de Inteligência Artificial;

VII – segurança no trabalho remoto e utilização de dispositivos móveis;

VIII – demais temas relevantes identificados na gestão de riscos.

A capacitação deverá ser especialmente considerada no ingresso de novos usuários e sempre que houver alteração relevante nos riscos, sistemas ou normas aplicáveis.

19. DESCUMPRIMENTO DA POLÍTICA

O descumprimento desta Política, das normas complementares ou dos procedimentos de segurança poderá ensejar a adoção das medidas administrativas, disciplinares, contratuais, civis ou penais cabíveis, observados a natureza do vínculo do usuário, a

legislação aplicável e, quando cabível, o devido processo legal, o contraditório e a ampla defesa.

A apuração de eventual descumprimento deverá considerar a natureza e a gravidade da conduta, a existência de dolo ou culpa, os danos causados, os riscos envolvidos e as circunstâncias do caso concreto.

20. GOVERNANÇA, REVISÃO E ATUALIZAÇÃO

A segurança da informação deverá ser tratada como responsabilidade compartilhada e elemento permanente de governança.

A SUPREV deverá promover o acompanhamento periódico dos riscos relacionados à segurança da informação e adotar medidas para seu tratamento e redução.

Esta Política deverá ser revisada, no mínimo, a cada quatro anos ou sempre que houver alteração relevante na legislação, nas normas superiores, nos processos institucionais, nos recursos tecnológicos ou nos riscos de segurança da informação.

As alterações deverão ser formalmente registradas, aprovadas pela autoridade competente e divulgadas aos usuários abrangidos por esta Política.

21. DISPOSIÇÕES FINAIS

Fica atualizada a Política Complementar de Segurança da Informação – PSI da Subsecretaria de Gestão Previdenciária – SUPREV, na forma estabelecida neste instrumento, ficando revogada a versão anterior da Política.

Esta Política possui caráter complementar à Política de Segurança da Informação da Prefeitura de Belo Horizonte e às normas, políticas, instruções normativas, padrões e procedimentos estabelecidos pelos órgãos competentes.

Na ausência de disposição específica nesta Política, deverão ser observadas as normas superiores aplicáveis.

Os requisitos estabelecidos nesta Política são obrigatórios para todos os usuários abrangidos por sua aplicação.

A segurança da informação constitui responsabilidade de todos os usuários, devendo integrar a cultura organizacional e as atividades cotidianas da SUPREV.

Belo Horizonte/MG, 10 de setembro de 2026.

ROBERTA ESTER SENNA PORTILHO MATOS:00361227698

Assinado de forma digital por ROBERTA ESTER SENNA PORTILHO MATOS:00361227698
Dados: 2026.09.10 15:05:35 -03'00'

ROBERTA ESTER SENNA PORTILHO MATOS

Diretora Central de Concessão de Benefícios Previdenciários - DCGB

Subsecretaria de Gestão Previdenciária e da Saúde do Segurado – SUPREV

WALLESKA MOREIRA SANTOS:81117078604

Assinado de forma digital por WALLESKA MOREIRA SANTOS:81117078604
Dados: 2026.09.10 15:10:21 -03'00'

WALLESKA MOREIRA SANTOS

Diretora de Compliance e Inteligência Previdenciária - DCIP

Subsecretaria de Gestão Previdenciária e da Saúde do Segurado – SUPREV

GLEISON PEREIRA DE SOUZA:82074313691

Assinado de forma digital por GLEISON PEREIRA DE SOUZA:82074313691
Dados: 2026.09.10 15:53:13 -03'00'

GLEISON PEREIRA DE SOUZA - BM 79.901-0

Subsecretário de Gestão Previdenciária e da Saúde do Segurado – SUPREV

Secretaria Municipal de Planejamento, Orçamento e Gestão – SMPOG – PBH