

SEPREV POLÍTICA DE SEGURANÇA DA INFORMAÇÃO – PSI

*Documento consolidado a partir da PSI existente, da proposta de atualização
e da Instrução Normativa SEPREV nº 02/2026.*

Documento	Política de Segurança da Informação – PSI
Instituição	SEPREV
Status	2º versão
Revisão	Versão revisada
Periodicidade prevista	A cada dois anos ou quando necessário

CAPÍTULO I – DISPOSIÇÕES PRELIMINARES

Art. 1º Esta Política de Segurança da Informação – PSI estabelece as diretrizes institucionais para a proteção das informações e dos ativos de informação do SEPREV, visando preservar sua confidencialidade, integridade, disponibilidade e autenticidade.

Art. 2º Esta Política aplica-se a todos os servidores, conselheiros, prestadores de serviço e terceiros que tenham acesso a informações, sistemas, equipamentos, redes ou demais ativos do SEPREV, independentemente do local em que as atividades sejam realizadas.

Art. 3º As disposições desta Política aplicam-se às informações em qualquer meio ou suporte, bem como aos recursos tecnológicos utilizados nas atividades institucionais.

Art. 4º A segurança da informação é responsabilidade de todos os usuários abrangidos por esta Política, que deverão conhecer, observar e cumprir as diretrizes e procedimentos aplicáveis às suas atividades.

Art. 5º O teletrabalho ou trabalho home office deverá observar, cumulativamente, esta Política e a Instrução Normativa SEPREV nº 02/2026, sem prejuízo de outras normas institucionais aplicáveis.

Art. 6º Toda informação produzida ou recebida pelos servidores como resultado da atividade profissional contratada pelo SEPREV pertence à instituição, observadas as disposições legais aplicáveis.

CAPÍTULO II – OBJETIVOS

Art. 7º São objetivos desta Política:

- I – proteger os ativos de informação do SEPREV;
- II – preservar a confidencialidade, integridade, disponibilidade e autenticidade das informações;
- III – reduzir os riscos de segurança da informação;
- IV – estabelecer responsabilidades e padrões de comportamento para usuários, gestores, fornecedores e terceiros;
- V – assegurar a utilização adequada dos recursos computacionais e dos serviços de Tecnologia da Informação;

- VI – apoiar a conformidade legal e institucional;
- VII – contribuir para a continuidade dos serviços;
- VIII – fortalecer a governança institucional e a cultura de segurança da informação;
- IX – estabelecer diretrizes para proteção de dados pessoais;
- X – estabelecer requisitos de segurança para atividades realizadas fora das dependências do SEPREV.

CAPÍTULO III – PRINCÍPIOS E DIRETRIZES GERAIS

Art. 8º A segurança da informação será orientada pelos princípios de confidencialidade, integridade, disponibilidade e autenticidade.

Art. 9º O acesso às informações e aos recursos tecnológicos deverá ser limitado às pessoas autorizadas e à necessidade decorrente de suas atribuições.

Art. 10. Os recursos tecnológicos e as informações institucionais deverão ser utilizados prioritariamente para as atividades do SEPREV. O uso pessoal eventualmente permitido não poderá prejudicar o desempenho dos sistemas e serviços, nem comprometer a segurança da informação.

Art. 11. As exceções às disposições desta Política deverão ser formalizadas, justificadas, avaliadas quanto aos riscos e autorizadas pela autoridade competente, permanecendo registradas pelo período definido pelo SEPREV.

CAPÍTULO IV – GOVERNANÇA E RESPONSABILIDADES

Art. 12. Fica instituído o Comitê de Segurança da Informação, responsável por deliberar sobre diretrizes de segurança da informação, avaliar riscos e acompanhar incidentes, no âmbito de suas competências.

Art. 13. A estrutura de governança de segurança da informação envolve, conforme suas atribuições institucionais:

- I – Presidência;
- II – Diretoria;
- III – Comitê de Segurança da Informação;
- IV – área de Tecnologia da Informação;
- V – Gestor de Segurança da Informação;

- VI – Encarregado pelo tratamento de dados pessoais;
- VII – gestores de pessoas e/ou processos;
- VIII – servidores, conselheiros, prestadores de serviço e terceiros.

Art. 14. Compete à Presidência:

- I – apoiar e patrocinar a segurança da informação;
- II – deliberar ou autorizar as matérias que dependam de sua competência;
- III – supervisionar o cumprimento das normas institucionais relacionadas ao teletrabalho, conforme a Instrução Normativa SEPREV nº 02/2026;
- IV – assegurar que esta Política seja aprovada pela autoridade competente.

Art. 15. Compete ao Comitê de Segurança da Informação:

- I – deliberar sobre diretrizes de segurança da informação;
- II – acompanhar os riscos de segurança da informação;
- III – acompanhar incidentes relevantes;
- IV – avaliar propostas de melhoria dos controles;
- V – apoiar a revisão desta Política.

Art. 16. Compete aos gestores de pessoas e/ou processos:

- I – atuar como referência de conduta para suas equipes;
- II – atribuir aos servidores e contratados a responsabilidade pelo cumprimento desta Política;
- III – exigir a ciência e o compromisso com as regras de segurança e confidencialidade;
- IV – adaptar processos e procedimentos sob sua responsabilidade aos requisitos desta Política;
- V – comunicar alterações de função, desligamentos e demais situações que possam exigir revisão ou revogação de acessos.

Art. 17. Compete à área de Tecnologia da Informação:

- I – configurar equipamentos, sistemas e ferramentas com os controles necessários;
- II – administrar, proteger e testar as cópias de segurança;
- III – realizar auditorias periódicas de configurações técnicas e análises de riscos;
- IV – implementar e manter controles de acesso;

- V – providenciar o bloqueio de acessos quando formalmente solicitado ou quando houver necessidade de medida restritiva para proteção dos ativos;
- VI – apoiar a resposta a incidentes;
- VII – promover ações de conscientização;
- VIII – apoiar a avaliação de controles de segurança para novos sistemas ou serviços;
- IX – planejar e monitorar capacidade de armazenamento, processamento e transmissão;
- X – testar a eficácia dos controles e informar riscos residuais aos gestores.

Art. 18. Compete ao Gestor de Segurança da Informação:

- I – coordenar as atividades relacionadas à segurança da informação;
- II – apoiar a gestão de riscos;
- III – acompanhar incidentes e ações corretivas;
- IV – acompanhar a aplicação desta Política;
- V – propor atualizações e melhorias nos controles.

Art. 19. Compete ao Encarregado pelo tratamento de dados pessoais atuar nas matérias relacionadas à proteção de dados pessoais, em articulação com a segurança da informação e com as áreas responsáveis pelo tratamento.

Art. 20. Compete aos servidores, conselheiros, prestadores de serviço e terceiros:

- I – cumprir esta Política e os procedimentos aplicáveis;
- II – proteger credenciais, equipamentos e informações sob sua responsabilidade;
- III – comunicar imediatamente incidentes, suspeitas de incidentes, perda, furto ou roubo de equipamentos;
- IV – utilizar somente recursos e meios autorizados;
- V – manter sigilo e confidencialidade das informações a que tenham acesso.

CAPÍTULO V – GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO

Art. 21. O SEPREV adotará metodologia estruturada de gestão de riscos de segurança da informação.

Art. 22. O processo de gestão de riscos deverá considerar, conforme aplicável:

- I – identificação dos ativos;
- II – identificação de ameaças e vulnerabilidades;
- III – avaliação de impacto;
- IV – avaliação da probabilidade;
- V – definição e avaliação de controles;
- VI – definição de tratamento;
- VII – registro dos riscos;
- VIII – avaliação do risco residual;
- IX – monitoramento e revisão periódica.

Art. 23. Os riscos deverão ser registrados em matriz específica e revisados periodicamente ou quando houver alteração relevante nos processos, sistemas, ativos, ameaças, vulnerabilidades ou requisitos institucionais.

Art. 24. O tratamento dos riscos deverá considerar medidas preventivas, detectivas e corretivas, conforme aplicável.

Art. 25. Os riscos residuais deverão ser comunicados aos gestores responsáveis para conhecimento e decisão quanto ao tratamento ou aceitação, conforme competência institucional.

CAPÍTULO VI – CLASSIFICAÇÃO DA INFORMAÇÃO

Art. 26. As informações do SEPREV serão classificadas, conforme sua natureza e necessidade de proteção, nos seguintes níveis:

- I – Pública;
- II – Interna;
- III – Restrita;
- IV – Confidencial.

Art. 27. A classificação deverá ser realizada no momento da criação ou recebimento da informação, sempre que aplicável.

Art. 28. Cada nível de classificação deverá observar controles compatíveis de acesso, armazenamento, transmissão, reprodução e descarte.

Art. 29. O responsável pela informação deverá promover a revisão da classificação quando houver alteração relevante de sua natureza, finalidade ou necessidade de proteção.

Art. 30. É vedada a divulgação, cópia, transmissão ou disponibilização de informação a pessoas não autorizadas, independentemente do meio utilizado.

CAPÍTULO VII – CONTROLE DE ACESSO E IDENTIDADE

Art. 31. O acesso aos sistemas, aplicações, equipamentos, bases de dados e informações deverá observar o princípio do menor privilégio e a necessidade de conhecimento.

Art. 32. Cada conta ou dispositivo de acesso deverá estar associado a responsável identificável como pessoa física.

Art. 33. É vedado o compartilhamento de senhas, contas, tokens ou outros mecanismos de autenticação pessoal.

Art. 34. As senhas deverão observar critérios de segurança definidos pela área de Tecnologia da Informação e deverão ser alteradas conforme os procedimentos institucionais aplicáveis.

Art. 35. Os acessos deverão ser revisados, no mínimo, semestralmente, ou imediatamente quando houver alteração de função, desligamento, afastamento ou mudança das atribuições do usuário.

Art. 36. O acesso poderá ser bloqueado ou revogado em razão de desligamento, alteração de função, incidente, investigação, descumprimento desta Política ou outra situação que exija medida restritiva para proteção dos ativos.

Art. 37. As funções administrativas e operacionais deverão ser segregadas sempre que tecnicamente e administrativamente aplicável, de forma a reduzir riscos decorrentes de privilégios excessivos.

CAPÍTULO VIII – SEGURANÇA FÍSICA E AMBIENTAL

Art. 38. O acesso físico às instalações do SEPREV deverá ser controlado conforme as regras institucionais aplicáveis.

Art. 39. Equipamentos e demais ativos de informação deverão ser protegidos contra danos, perda, furto, roubo e acesso não autorizado.

Art. 40. O acesso ao Datacenter deverá ocorrer por mecanismo de autenticação ou controle de acesso adequado, sendo o acesso de visitantes ou terceiros acompanhado por servidor autorizado, conforme as regras existentes do SEPREV.

Art. 41. O Datacenter deverá ser mantido limpo e organizado, observadas as restrições existentes quanto à entrada de alimentos, bebidas e produtos que possam comprometer a segurança do ambiente.

CAPÍTULO IX – MESA LIMPA E TELA LIMPA

Art. 42. Documentos, mídias, informações e demais materiais institucionais deverão ser mantidos de forma a impedir acesso, visualização, cópia ou utilização por pessoas não autorizadas.

Art. 43. O usuário deverá bloquear o equipamento sempre que se ausentar do posto de trabalho.

Art. 44. Em atividades realizadas fora das dependências do SEPREV, inclusive em teletrabalho, o usuário deverá adotar medidas para impedir a visualização ou acesso indevido às informações institucionais.

CAPÍTULO X – SEGURANÇA DE DISPOSITIVOS E ATIVOS FORA DAS INSTALAÇÕES

Art. 45. Computadores, notebooks, smartphones, mídias removíveis e demais dispositivos institucionais deverão ser utilizados de acordo com as regras estabelecidas pela área de Tecnologia da Informação.

Art. 46. Não será permitida alteração da configuração de sistemas operacionais, mecanismos de segurança ou geração de logs sem comunicação e autorização da área de Tecnologia da Informação.

Art. 47. É vedada a instalação ou utilização de programas e aplicativos não autorizados pela área de Tecnologia da Informação.

Art. 48. Os dispositivos institucionais utilizados fora das instalações deverão permanecer sob guarda e responsabilidade do usuário autorizado e protegidos contra acesso não autorizado, perda, furto, roubo ou dano.

Art. 49. A ocorrência de furto, roubo, perda ou comprometimento de dispositivo institucional deverá ser comunicada imediatamente ao gestor e à área de Tecnologia da Informação.

CAPÍTULO XI – SEGURANÇA NO HOME OFFICE E TELETRABALHO

Art. 50. O trabalho em regime de home office ou teletrabalho deverá observar integralmente esta Política e a Instrução Normativa SEPREV nº 02/2026.

Art. 51. O servidor em teletrabalho deverá manter ambiente adequado e seguro para execução das atividades, conexão estável à internet e equipamentos compatíveis com os sistemas institucionais, observadas as responsabilidades estabelecidas na Instrução Normativa SEPREV nº 02/2026.

Art. 52. O acesso aos sistemas institucionais durante o teletrabalho deverá ocorrer por redes seguras e por meios autorizados pelo SEPREV.

Art. 53. É obrigatória a utilização de senha pessoal e intransferível e é vedado o compartilhamento de credenciais, equipamentos, sessões ou dados institucionais com terceiros.

Art. 54. Os equipamentos utilizados no teletrabalho deverão possuir os mecanismos de proteção definidos pelo SEPREV, incluindo antivírus atualizado quando aplicável.

Art. 55. O servidor deverá impedir que familiares, visitantes ou terceiros tenham acesso, visualização, cópia ou utilização das informações institucionais.

Art. 56. É vedado o armazenamento ou transmissão de informações institucionais por meios não autorizados pelo SEPREV.

Art. 57. O usuário deverá bloquear o equipamento sempre que se ausentar do local de trabalho, inclusive durante o teletrabalho.

Art. 58. O servidor deverá zelar pela guarda, conservação e uso adequado dos equipamentos institucionais eventualmente disponibilizados pelo SEPREV.

Art. 59. Qualquer incidente de segurança, suspeita de comprometimento, perda, furto ou roubo de equipamento, credencial ou informação deverá ser comunicado imediatamente à Administração, ao gestor responsável e à área competente de

Tecnologia da Informação, sem prejuízo da comunicação ao Encarregado quando houver dados pessoais envolvidos.

Art. 60. O regime de teletrabalho será concedido, acompanhado, avaliado e revogado conforme a Instrução Normativa SEPREV nº 02/2026 e demais normas aplicáveis.

CAPÍTULO XII – SEGURANÇA DE REDES E COMUNICAÇÕES

Art. 61. O acesso aos sistemas e serviços institucionais deverá utilizar mecanismos de comunicação e rede autorizados pelo SEPREV.

Art. 62. Redes utilizadas para acesso institucional fora das instalações deverão possuir condições de segurança compatíveis com a atividade realizada.

Art. 63. É vedado utilizar redes ou meios de comunicação que possam comprometer a confidencialidade, integridade ou disponibilidade das informações institucionais.

Art. 64. A área de Tecnologia da Informação poderá implementar mecanismos de monitoramento e proteção das redes, sistemas, estações de trabalho, dispositivos móveis, correio eletrônico e conexões com a Internet, observadas as leis brasileiras e as regras institucionais aplicáveis.

CAPÍTULO XIII – TRANSFERÊNCIA DE INFORMAÇÕES

Art. 65. A transferência de informações deverá ocorrer somente para destinatários autorizados e mediante meios aprovados pelo SEPREV.

Art. 66. Antes da transferência, deverão ser considerados a classificação da informação, a necessidade do destinatário e os riscos associados ao meio utilizado.

Art. 67. É vedado utilizar serviços pessoais, aplicações não autorizadas ou outros meios não aprovados para transferir informações institucionais.

CAPÍTULO XIV – PROTEÇÃO DE DADOS PESSOAIS E PRIVACIDADE

Art. 68. O tratamento de dados pessoais realizado pelo SEPREV deverá observar a Lei nº 13.709/2018 – LGPD e demais requisitos legais aplicáveis.

Art. 69. Deverão ser adotadas medidas técnicas e administrativas para proteção dos dados pessoais contra acessos não autorizados e situações acidentais ou ilícitas.

Art. 70. O acesso a dados pessoais deverá ser limitado às pessoas autorizadas e à necessidade decorrente de suas atribuições.

Art. 71. O compartilhamento de dados pessoais deverá observar a finalidade institucional, a necessidade do tratamento e os requisitos legais e administrativos aplicáveis.

Art. 72. Incidentes envolvendo dados pessoais deverão ser comunicados imediatamente ao responsável pela segurança da informação e ao Encarregado pelo tratamento de dados pessoais, para avaliação e adoção das providências cabíveis.

Art. 73. A proteção de dados pessoais deverá ser considerada nos processos de desenvolvimento, aquisição, alteração ou contratação de sistemas e serviços que realizem tratamento de dados pessoais.

CAPÍTULO XV – USO DE CORREIO ELETRÔNICO E INTERNET

Art. 74. O correio eletrônico institucional deverá ser utilizado para atividades relacionadas às atribuições do SEPREV, observadas as regras específicas de uso estabelecidas pela instituição.

Art. 75. É vedado utilizar o correio eletrônico institucional para:

- I – divulgar informações não autorizadas;
- II – utilizar a identidade ou endereço eletrônico de outra pessoa sem autorização;
- III – enviar conteúdo que exponha o SEPREV a riscos legais ou de segurança;
- IV – buscar acesso não autorizado a computadores, servidores ou redes;
- V – burlar mecanismos de segurança;
- VI – disseminar código malicioso ou arquivos que representem risco à segurança;
- VII – acessar ou divulgar informações confidenciais sem autorização.

Art. 76. A utilização da Internet deverá observar padrões legais, éticos e de segurança, sendo vedadas atividades que comprometam os sistemas, serviços, informações ou a imagem institucional do SEPREV.

CAPÍTULO XVI – GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

Art. 77. Todo incidente ou suspeita de incidente de segurança da informação deverá ser comunicado imediatamente por meio do canal institucional definido pelo SEPREV.

Art. 78. Os incidentes deverão ser registrados, classificados, analisados, tratados e acompanhados até seu encerramento.

Art. 79. A resposta ao incidente deverá considerar sua criticidade e os impactos potenciais sobre a confidencialidade, integridade, disponibilidade e autenticidade das informações.

Art. 80. Após o tratamento do incidente deverão ser registradas, quando aplicável:

- I – causa identificada;
- II – evidências relevantes;
- III – medidas adotadas;
- IV – impactos observados;
- V – ações corretivas e preventivas;
- VI – necessidade de atualização dos controles ou procedimentos.

Art. 81. Incidentes envolvendo dados pessoais deverão ser tratados também em articulação com o Encarregado pelo tratamento de dados pessoais.

CAPÍTULO XVII – CONTINUIDADE E RECUPERAÇÃO

Art. 82. O SEPREV deverá manter procedimentos de backup e restauração dos dados e sistemas considerados críticos ou relevantes.

Art. 83. Os backups deverão ser realizados por mecanismos de agendamento e controle compatíveis com a criticidade dos dados e sistemas.

Art. 84. Os backups deverão possuir cópias protegidas e, quando aplicável, mantidas em local ou infraestrutura distinta do ambiente principal.

Art. 85. Deverão ser realizados testes periódicos de restauração para verificar a capacidade de recuperação dos dados.

Art. 86. O SEPREV deverá estabelecer estratégias e planos de continuidade e recuperação de desastres para processos e serviços críticos, considerando

indisponibilidade de pessoas, instalações, equipamentos, sistemas, redes, dados e fornecedores.

Art. 87. Os planos de continuidade e recuperação deverão ser periodicamente testados, avaliados e atualizados.

Art. 88. O teletrabalho poderá ser considerado, quando aplicável e autorizado, entre as alternativas operacionais para manutenção de atividades durante situações que impeçam ou restrinjam o trabalho presencial, observadas a Instrução Normativa SEPREV nº 02/2026, os riscos identificados e os requisitos de segurança desta Política.

CAPÍTULO XVIII – MONITORAMENTO, LOGS E AUDITORIA

Art. 89. O SEPREV poderá implementar mecanismos de monitoramento em estações de trabalho, servidores, correio eletrônico, conexões com a Internet, dispositivos móveis, redes e demais componentes tecnológicos, observadas as leis brasileiras.

Art. 90. Deverão ser mantidos logs e trilhas de auditoria dos sistemas e serviços conforme sua necessidade e criticidade.

Art. 91. Os registros de auditoria deverão ser protegidos contra alteração ou exclusão não autorizada.

Art. 92. Auditorias e avaliações de conformidade poderão ser realizadas periodicamente, conforme planejamento institucional ou necessidade identificada.

Art. 93. Os resultados de auditorias, avaliações de riscos e incidentes relevantes deverão subsidiar ações corretivas e melhorias dos controles.

CAPÍTULO XIX – CAPACITAÇÃO E CONSCIENTIZAÇÃO

Art. 94. O SEPREV deverá promover capacitação e conscientização em segurança da informação e proteção de dados pessoais.

Art. 95. Os treinamentos deverão contemplar, conforme aplicável:

- I – proteção de credenciais;
- II – uso seguro de equipamentos;
- III – proteção de informações;
- IV – segurança no teletrabalho;

- V – prevenção e comunicação de incidentes;
- VI – proteção de dados pessoais;
- VII – uso seguro de correio eletrônico e Internet.

Art. 96. Deverão ser realizadas ações de integração e reciclagem sempre que necessário, observadas as necessidades institucionais.

CAPÍTULO XX – SANÇÕES E DESCUMPRIMENTO

Art. 97. O descumprimento desta Política deverá ser apurado de acordo com os procedimentos administrativos e legais aplicáveis.

Art. 98. Conforme a natureza e a gravidade da ocorrência, poderão ser adotadas medidas administrativas, disciplinares, contratuais ou outras providências previstas na legislação e nas normas institucionais aplicáveis.

Art. 99. A adoção de medidas em razão de violação desta Política deverá considerar, conforme aplicável, a natureza da ocorrência, a intenção, a negligência, o acidente, o desconhecimento, o impacto causado e os riscos envolvidos.

Art. 100. O acesso a sistemas ou recursos poderá ser bloqueado ou cancelado quando necessário para proteger os ativos do SEPREV, sem prejuízo das demais medidas administrativas cabíveis.

CAPÍTULO XXI – GESTÃO DE FORNECEDORES E TERCEIROS

Art. 101. Fornecedores, prestadores de serviço e terceiros que tenham acesso a informações ou recursos do SEPREV deverão observar esta Política e os requisitos de segurança aplicáveis às atividades contratadas.

Art. 102. As responsabilidades de segurança, sigilo e confidencialidade deverão ser formalizadas nos instrumentos aplicáveis, quando cabível.

Art. 103. Os acessos concedidos a terceiros deverão ser limitados ao necessário para execução das atividades autorizadas e deverão ser revogados quando deixarem de ser necessários.

CAPÍTULO XXII – REVISÃO, APROVAÇÃO E CONTROLE DA POLÍTICA

Art. 104. Esta Política deverá ser revisada, no mínimo, a cada dois anos ou sempre que ocorrer:

- I – alteração significativa na estrutura organizacional;
- II – alteração relevante nos processos ou sistemas;
- III – mudança significativa no perfil de riscos;
- IV – alteração relevante na legislação ou nos requisitos aplicáveis;
- V – ocorrência de incidente que indique necessidade de atualização;
- VI – alteração relevante no regime de trabalho ou nas tecnologias utilizadas.

Art. 105. A revisão deverá ser precedida de análise pelo responsável pela segurança da informação e pelas áreas competentes, conforme a matéria.

Art. 106. A versão revisada deverá ser submetida à aprovação do órgão superior competente.

Art. 107. As alterações aprovadas deverão ser registradas, controladas por versão e divulgadas aos usuários abrangidos por esta Política.

Art. 108. Os usuários deverão manter-se atualizados em relação a esta Política e aos procedimentos e normas relacionados, buscando orientação do gestor ou da área de Tecnologia da Informação quando houver dúvida quanto ao uso, proteção, transferência ou descarte de informações.

CAPÍTULO XXIII – DISPOSIÇÕES FINAIS

Art. 109. Os casos omissos serão submetidos à autoridade competente do SEPREV, observadas as atribuições institucionais e as normas aplicáveis.

Art. 110. Esta Política deverá ser observada integralmente por todos os usuários abrangidos por seu escopo.

Art. 111. Esta Política deverá ser mantida em versão controlada e disponibilizada aos usuários pelos meios institucionais definidos pelo SEPREV.

Art. 112. Integram o contexto de aplicação desta Política, no que couber, a Instrução Normativa SEPREV nº 02/2026 e os procedimentos institucionais relacionados à segurança da informação, proteção de dados, gestão de riscos, continuidade, acesso e uso dos recursos tecnológicos.

Elias Alves

Presidente Executivo

ANEXO I – TERMO DE CIÊNCIA E COMPROMISSO

***TERMO DE CIÊNCIA E COMPROMISSO DA POLÍTICA DE
SEGURANÇA DA INFORMAÇÃO – PSI DO SEPREV***

Declaro que recebi, li e estou ciente das disposições da Política de Segurança da Informação – PSI do SEPREV e comprometo-me a observar integralmente as regras aplicáveis às minhas atividades, incluindo as disposições relacionadas à proteção das informações, segurança dos recursos tecnológicos, proteção de dados pessoais, gestão de incidentes e trabalho em regime de teletrabalho, quando aplicável.

Declaro, ainda, estar ciente da responsabilidade de comunicar imediatamente incidentes, suspeitas de incidentes, perda, furto, roubo ou comprometimento de equipamentos, credenciais ou informações institucionais.

Franco da Rocha, _____ de _____ de _____.

Nome completo:

Matrícula:

Cargo:

Assinatura:

**ANEXO II – REQUISITOS MÍNIMOS DE SEGURANÇA PARA
TELETRABALHO**

1. Ambiente de trabalho adequado e seguro.
2. Conexão estável à Internet.
3. Equipamento compatível com os sistemas institucionais.
4. Senha pessoal e intransferível.
5. Antivírus atualizado, quando aplicável.
6. Utilização de redes seguras.
7. Proibição de compartilhamento de dados institucionais.
8. Proteção física do equipamento.
9. Bloqueio da tela durante ausências.
10. Impedimento de acesso de terceiros às informações institucionais.
11. Comunicação imediata de incidentes.
12. Observância integral da PSI e da Instrução Normativa SEPREV nº 02/2026.

ANEXO III – MATRIZ DE CORRESPONDÊNCIA DE CONTROLES

A presente Política de Segurança da Informação deverá possuir Matriz de Correspondência de Controles, mantida como documento controlado e atualizada sempre que houver alteração relevante nesta Política, nos procedimentos internos ou nos referenciais normativos adotados.

A matriz deverá relacionar, quando aplicáveis, os requisitos da ISO/IEC 27001:2022 e os controles da ISO/IEC 27002:2022 às disposições desta Política, aos procedimentos internos correspondentes e às respectivas evidências de implementação.

Os controles cuja aplicabilidade, implementação ou evidência ainda não tenha sido formalmente validada deverão ser identificados como “[verificar]”, até a conclusão da respectiva análise.



SERVIÇO MUNICIPAL DE PREVIDÊNCIA SOCIAL SEPREV

C.N.P.J. 96.493.648/0001-16

Assinado por 1 pessoa: ELIAS ALVES
Para verificar a validade das assinaturas, acesse <https://seprevfrancodarocha.1doc.com.br/verificacao/29CB-A254-43C1-A499> e informe o código 29CB-A254-43C1-A499





VERIFICAÇÃO DAS ASSINATURAS



Código para verificação: 29CB-A254-43C1-A499

Este documento foi assinado digitalmente pelos seguintes signatários nas datas indicadas:



ELIAS ALVES (CPF 084.XXX.XXX-30) em 29/09/2026 09:46:18 GMT-03:00

Papel: Parte

Emitido por: Sub-Autoridade Certificadora 1Doc (Assinatura 1Doc)



ELIAS ALVES (CPF 084.XXX.XXX-30) em 29/09/2026 09:53:26 GMT-03:00

Papel: Parte

Emitido por: Sub-Autoridade Certificadora 1Doc (Assinatura 1Doc)

Para verificar a validade das assinaturas, acesse a Central de Verificação por meio do link:

<https://seprevfrancodarocha.1doc.com.br/verificacao/29CB-A254-43C1-A499>