



ESTADO DO RIO GRANDE DO SUL
MUNICÍPIO DE TRÊS PASSOS/RS
**INSTITUTO DE PREVIDÊNCIA DOS SERVIDORES
PÚBLICOS DO MUNICÍPIO DE TRÊS PASSOS**



MANUALIZAÇÃO DA SEGURANÇA DA INFORMAÇÃO

CNPJ: 04.510.687/0001-66

Av. Santos Dumont, nº75 – Bairro Centro – Três Passos/RS – CEP 98600-000



Assinado com Assinatura Eletrônica (Lei 14.063/2020 | Regulamento 910/2014/EC)

Hash SHA256 do original: 8272248c570b5600c2903383d04849a9dd69c07983e2cb73aedfcacf3393b9e9

Link de validação: <https://valida.ae/bb8779dc2c31063abfb49f465810be045a7ca97a3cc456f8f>





Sumário

MANUALIZAÇÃO DA SEGURANÇA DA INFORMAÇÃO	1
1. OBJETIVO.....	4
2. FUNDAMENTAÇÃO LEGAL E NORMATIVA	4
3. CONCEITOS	5
4. RESPONSABILIDADES.....	6
4.1. Da Diretoria Executiva	6
4.2. Da Área ou do Responsável pela Tecnologia da Informação.....	6
4.3. Dos Usuários	7
4.4. Dos Prestadores de Serviços e Terceiros.....	7
5. GESTÃO DE ACESSOS E IDENTIFICAÇÃO	7
5.1. Solicitação e Criação de Acesso	7
5.2. Senhas e Credenciais	8
5.3. Alteração e Recuperação de Senha.....	8
5.4. Bloqueio e Exclusão de Acessos.....	8
6. UTILIZAÇÃO DE COMPUTADORES E RECURSOS TECNOLÓGICOS.....	9
6.1. Instalação de Programas	9
6.2. Armazenamento dos Documentos	9
6.3. Bloqueio das Estações	9
6.4. Manutenção dos Equipamentos	9
7. USO DO CORREIO ELETRÔNICO E DA INTERNET	10
7.1. Correio Eletrônico	10
7.2. Internet.....	10





ESTADO DO RIO GRANDE DO SUL
MUNICÍPIO DE TRÊS PASSOS/RS
**INSTITUTO DE PREVIDÊNCIA DOS SERVIDORES
PÚBLICOS DO MUNICÍPIO DE TRÊS PASSOS**



8. TRATAMENTO E PROTEÇÃO DE DOCUMENTOS FÍSICOS.....	10
8.1. Consulta e Retirada.....	10
8.2. Devolução	11
9. DISPOSITIVOS MÓVEIS	11
10. <i>PROCEDIMENTOS DE CONTINGÊNCIA</i>	11
11. BACKUP E RECUPERAÇÃO DAS INFORMAÇÕES.....	16
12. MONITORAMENTO E AUDITORIA	16
13. GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO	17
14. PROTEÇÃO E PRIVACIDADE DAS INFORMAÇÕES.....	17
15. CONSCIENTIZAÇÃO DOS USUÁRIOS	18
16. REGISTROS E EVIDÊNCIAS	18
17. TERMO DE CIÊNCIA E COMPROMISSO	18
18. REVISÃO E ATUALIZAÇÃO.....	19
19. DISPOSIÇÕES FINAIS.....	19

CNPJ: 04.510.687/0001-66

Av. Santos Dumont, nº75 – Bairro Centro – Três Passos/RS – CEP 98600-000



Assinado com Assinatura Eletrônica (Lei 14.063/2020 | Regulamento 910/2014/EC)
Hash SHA256 do original: 8272248c570b5600c2903383d04849a9dd69c07983e2cb73aedfcacf3393b9e9
Link de validação: <https://valida.ae/bb8779dc2c31063abfb49f465810be045a7ca97a3cc456f8f>





1. OBJETIVO

Este Manual de Segurança da Informação tem por objetivo estabelecer, de forma clara e padronizada, os procedimentos operacionais relacionados à proteção, utilização, armazenamento, acesso, compartilhamento e preservação das informações e dos recursos tecnológicos do Instituto de Previdência dos Servidores Públicos do Município de Três Passos – IP3P.

O Manual complementa a Política de Segurança da Informação – PSI do IP3P, convertendo suas diretrizes em procedimentos aplicáveis às rotinas administrativas da Autarquia, de modo a assegurar a confidencialidade, integridade e disponibilidade das informações institucionais.

São objetivos específicos deste Manual:

- a) padronizar os procedimentos relacionados à segurança da informação;
- b) definir responsabilidades quanto ao acesso, utilização e proteção das informações e dos recursos tecnológicos;
- c) estabelecer procedimentos para concessão, alteração, bloqueio e encerramento de acessos;
- d) orientar a utilização adequada dos equipamentos, sistemas, correio eletrônico, internet e dispositivos móveis;
- e) estabelecer controles para proteção de documentos e informações em meio físico e digital;
- f) disciplinar os procedimentos de backup, monitoramento e resposta a situações que possam comprometer a segurança das informações;
- g) assegurar a existência de registros e evidências suficientes para acompanhamento, controle e auditoria dos procedimentos adotados.

A Política de Segurança da Informação do IP3P reconhece a informação como ativo de relevante valor institucional e estabelece como princípios essenciais sua integridade, confidencialidade e disponibilidade.

2. FUNDAMENTAÇÃO LEGAL E NORMATIVA

Os procedimentos previstos neste Manual deverão ser executados em conformidade com a legislação vigente, com a Política de Segurança da Informação do IP3P e com os demais atos normativos aplicáveis à Administração Pública e aos Regimes Próprios de Previdência Social.

Constituem referências para aplicação deste Manual, especialmente:

I – a Constituição Federal;

II – a Lei Federal nº 9.717, de 27 de novembro de 1998, que estabelece regras gerais para organização e funcionamento dos Regimes Próprios de Previdência Social;

CNPJ: 04.510.687/0001-66

Av. Santos Dumont, nº75 – Bairro Centro – Três Passos/RS – CEP 98600-000



12





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

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

V – a Portaria MTP nº 1.467, de 2 de junho de 2022, e suas alterações;

VI – as normas e orientações expedidas pela Secretaria de Regime Próprio e Complementar do Ministério da Previdência Social;

VII – o Manual do Pró-Gestão RPPS aplicável ao nível de certificação adotado pelo IP3P;

VIII – as normas técnicas de segurança da informação adotadas como referência pela Política de Segurança da Informação do Instituto;

IX – a Política de Segurança da Informação – PSI do IP3P;

X – as demais políticas, manuais, normas internas e atos administrativos relacionados à governança, proteção de dados, tecnologia da informação e gestão documental do IP3P.

A Política de Segurança da Informação do Instituto adota como referência técnica as recomendações da ABNT NBR ISO/IEC 27002.

3. CONCEITOS

Para fins deste Manual, consideram-se:

I – Informação: conjunto de dados, documentos, registros ou conhecimentos produzidos, recebidos, armazenados ou utilizados pelo IP3P, independentemente do meio em que se encontrem.

II – Ativo de Informação: qualquer informação, sistema, equipamento, documento, banco de dados, recurso tecnológico ou outro elemento que possua valor para o IP3P e necessite de proteção.

III – Confidencialidade: garantia de que a informação somente seja acessada por pessoas devidamente autorizadas.

IV – Integridade: garantia de manutenção da informação em seu estado adequado, protegendo-a contra alterações indevidas, acidentais ou intencionais.

V – Disponibilidade: garantia de que a informação e os recursos correspondentes estejam disponíveis aos usuários autorizados sempre que necessários.

VI – Usuário: servidor, estagiário, prestador de serviço, fornecedor ou qualquer pessoa autorizada a utilizar informações, sistemas ou recursos tecnológicos do IP3P.





VII – Credencial de acesso: mecanismo destinado à identificação e autenticação de usuário, compreendendo login, senha, certificado digital, assinatura digital ou outro mecanismo equivalente.

VIII – Backup: cópia de segurança de dados e informações destinada à sua recuperação em caso de perda, indisponibilidade, exclusão, falha ou incidente.

IX – Incidente de Segurança da Informação: evento que possa comprometer ou efetivamente comprometa a confidencialidade, integridade ou disponibilidade das informações ou dos recursos tecnológicos do Instituto.

X – Dispositivo móvel: equipamento eletrônico portátil utilizado para acesso, armazenamento ou transmissão de informações, incluindo notebooks, smartphones e dispositivos de armazenamento removíveis.

XI – Log: registro eletrônico de eventos e atividades realizadas em sistemas, equipamentos, redes ou serviços tecnológicos.

4. RESPONSABILIDADES

A segurança da informação constitui responsabilidade compartilhada entre todos os agentes que tenham acesso às informações e aos recursos do IP3P.

4.1. Da Diretoria Executiva

Compete à Diretoria Executiva:

- a) assegurar a implementação e o cumprimento da Política de Segurança da Informação e deste Manual;
- b) deliberar sobre situações que demandem autorização superior;
- c) assegurar, dentro das possibilidades administrativas do Instituto, a disponibilização dos recursos necessários à proteção das informações;
- d) determinar a adoção de medidas corretivas quando identificadas fragilidades ou descumprimentos;
- e) promover a integração entre segurança da informação, proteção de dados, gestão documental e governança institucional.

4.2. Da Área ou do Responsável pela Tecnologia da Informação

Compete à equipe, empresa contratada ou profissional responsável pela tecnologia da informação, conforme a estrutura adotada pelo IP3P:

- a) configurar e manter os controles tecnológicos necessários;
- b) criar, alterar, bloquear e excluir acessos quando formalmente solicitado ou autorizado;
- c) adotar mecanismos de proteção dos equipamentos e sistemas;

CNPJ: 04.510.687/0001-66

Av. Santos Dumont, nº75 – Bairro Centro – Três Passos/RS – CEP 98600-000





- d) administrar e testar as cópias de segurança;
- e) manter, quando tecnicamente disponível, registros de acesso e logs;
- f) comunicar à Diretoria situações que representem risco à segurança da informação;
- g) prestar suporte na avaliação de incidentes;
- h) realizar as manutenções e alterações de configuração autorizadas;
- i) observar a segregação de funções e limitar privilégios ao mínimo necessário.

A PSI atribui à área de tecnologia, entre outras responsabilidades, a configuração dos equipamentos, proteção e teste das cópias de segurança, gestão das contas de acesso, auditoria das configurações e bloqueio de usuários quando necessário.

4.3. Dos Usuários

Todo usuário deverá:

- a) utilizar os recursos institucionais exclusivamente de forma compatível com suas atribuições;
- b) preservar suas credenciais de acesso;
- c) não compartilhar senhas ou outros mecanismos pessoais de identificação;
- d) proteger documentos e informações sob sua responsabilidade;
- e) comunicar situações suspeitas ou incidentes de segurança;
- f) respeitar as restrições de acesso estabelecidas;
- g) observar a Política de Segurança da Informação e este Manual.

4.4. Dos Prestadores de Serviços e Terceiros

Os prestadores de serviços que tenham acesso a informações, sistemas ou recursos tecnológicos do IP3P deverão observar as mesmas regras de segurança aplicáveis aos usuários internos, naquilo que for pertinente às atividades contratadas.

O acesso deverá limitar-se às informações e recursos necessários à execução dos serviços, podendo ser revogado quando cessada a necessidade que justificou sua concessão.

5. GESTÃO DE ACESSOS E IDENTIFICAÇÃO

Os acessos aos sistemas, equipamentos, bancos de dados e demais ativos de informação deverão ser concedidos de acordo com a necessidade funcional do usuário, respeitando-se o princípio do menor privilégio.

5.1. Solicitação e Criação de Acesso

A criação de novo acesso deverá decorrer da necessidade de execução das atividades institucionais.

Sempre que possível, cada usuário deverá possuir identificação individual, vinculada à pessoa física responsável por sua utilização.



A criação do acesso será realizada pela área ou responsável técnico competente, de acordo com as permissões necessárias às atribuições do usuário.

A PSI determina que as contas ou dispositivos de acesso sejam atribuídos a responsáveis identificáveis e estabelece responsabilidade individual sobre os logins.

5.2. Senhas e Credenciais

As senhas são pessoais e deverão ser mantidas sob sigilo.

É vedado:

- a) compartilhar senhas;
- b) utilizar credencial pertencente a outro usuário;
- c) permitir que terceiros utilizem credenciais pessoais;
- d) armazenar senhas de forma ostensiva ou facilmente acessível;
- e) compartilhar logins destinados à administração de sistemas.

No primeiro acesso, quando o sistema permitir, o usuário deverá substituir a senha inicialmente fornecida.

A PSI estabelece que os dispositivos de identificação devem estar associados a uma única pessoa física e veda seu compartilhamento.

5.3. Alteração e Recuperação de Senha

Caso haja suspeita de comprometimento da senha, o usuário deverá providenciar sua alteração imediatamente ou solicitar auxílio ao responsável técnico.

Na hipótese de esquecimento ou impossibilidade de acesso, a redefinição deverá ser solicitada ao responsável competente, que realizará a recuperação ou cadastramento de nova senha conforme os mecanismos disponíveis.

5.4. Bloqueio e Exclusão de Acessos

Os acessos deverão ser bloqueados ou excluídos quando:

- a) deixarem de ser necessários;
- b) ocorrer desligamento ou exoneração;
- c) encerrar-se contrato ou prestação de serviço;
- d) houver mudança de atribuições que elimine a necessidade do acesso;
- e) houver suspeita de comprometimento da credencial;
- f) houver determinação administrativa decorrente de incidente ou investigação.

A PSI determina expressamente que acessos desnecessários sejam imediatamente bloqueados.



6. UTILIZAÇÃO DE COMPUTADORES E RECURSOS TECNOLÓGICOS

Os computadores, equipamentos e demais recursos tecnológicos disponibilizados pelo IP3P destinam-se prioritariamente à execução das atividades institucionais.

Cada usuário será responsável pela adequada utilização dos equipamentos que lhe forem disponibilizados.

Não poderão ser realizadas alterações físicas ou lógicas, instalações, desinstalações ou modificações de configuração sem conhecimento ou autorização da área responsável pela tecnologia da informação.

6.1. Instalação de Programas

A instalação de programas deverá ocorrer somente quando necessária às atividades do IP3P e mediante autorização ou execução pelo responsável técnico.

Não deverão ser instalados softwares sem licença regular, programas de procedência desconhecida ou aplicações que possam comprometer a segurança dos equipamentos e da rede.

6.2. Armazenamento dos Documentos

Os documentos relevantes às atividades institucionais deverão ser armazenados nos locais oficiais definidos pelo IP3P, especialmente em servidor, sistema institucional, unidade de rede ou solução equivalente sujeita aos mecanismos de proteção e backup adotados.

Documentos armazenados exclusivamente no computador local poderão não estar abrangidos pelos procedimentos de backup.

Essa orientação já consta expressamente da PSI do Instituto.

6.3. Bloqueio das Estações

Ao se afastar do computador, o usuário deverá bloquear a estação de trabalho, evitando o acesso por pessoa não autorizada.

Sempre que possível, os equipamentos deverão possuir mecanismos automáticos de bloqueio após período de inatividade.

6.4. Manutenção dos Equipamentos

A manutenção física ou lógica dos equipamentos deverá ser realizada pela área de tecnologia da informação ou por prestador devidamente autorizado.

Caso o equipamento necessite ser encaminhado a terceiro, deverão ser adotadas medidas compatíveis com a proteção das informações nele armazenadas.





7. USO DO CORREIO ELETRÔNICO E DA INTERNET

O correio eletrônico e a internet constituem recursos destinados ao desenvolvimento das atividades institucionais e deverão ser utilizados de maneira ética, responsável e segura.

7.1. Correio Eletrônico

O usuário deverá:

- a) utilizar preferencialmente o correio eletrônico institucional nas comunicações oficiais;
- b) conferir destinatários antes do envio de informações;
- c) ter cautela com links, anexos e mensagens de origem desconhecida;
- d) evitar encaminhar informações institucionais a pessoas não autorizadas;
- e) não utilizar credenciais ou endereço eletrônico de outro usuário;
- f) comunicar mensagens suspeitas quando houver risco à segurança.

A PSI contém regras específicas para utilização do correio eletrônico, inclusive quanto à divulgação não autorizada de documentos, utilização indevida de identidade e envio de conteúdos capazes de comprometer a segurança.

7.2. Internet

O acesso à internet deverá observar as necessidades das atividades institucionais e não poderá ser utilizado para práticas ilícitas ou que comprometam a segurança da rede.

É vedada a utilização dos recursos do Instituto para tentar obter acesso não autorizado a sistemas, burlar mecanismos de segurança, disseminar códigos maliciosos ou compartilhar indevidamente informações institucionais.

O IP3P poderá adotar mecanismos de monitoramento, registro ou bloqueio de acessos, nos termos da Política de Segurança da Informação.

8. TRATAMENTO E PROTEÇÃO DE DOCUMENTOS FÍSICOS

Os documentos físicos que contenham informações de acesso restrito deverão ser armazenados em locais que permitam controle adequado e evitem acesso por pessoas não autorizadas.

8.1. Consulta e Retirada

A consulta ou retirada de documentos sujeitos a controle deverá ser acompanhada pelo responsável designado.

Quando houver retirada temporária, deverá ser emitido protocolo contendo, no mínimo:

- a) identificação do responsável pela liberação;
- b) identificação da pessoa que realizou a retirada ou consulta;

CNPJ: 04.510.687/0001-66

Av. Santos Dumont, nº75 – Bairro Centro – Três Passos/RS – CEP 98600-000





- c) data e hora da retirada ou consulta;
- d) data e hora da devolução.

A PSI estabelece expressamente esse procedimento para informações sensíveis mantidas em meio físico.

8.2. Devolução

No momento da devolução, o responsável deverá verificar a integridade e organização dos documentos.

Constatada ausência de folha, rasura, dano ou outra irregularidade relevante, a ocorrência deverá ser registrada e comunicada ao responsável competente.

9. DISPOSITIVOS MÓVEIS

O uso de notebooks, smartphones, pendrives e outros dispositivos móveis para atividades institucionais deverá observar os mesmos requisitos de segurança aplicáveis aos demais recursos tecnológicos.

O usuário deverá:

- a) manter o dispositivo protegido contra acesso indevido;
- b) evitar armazenamento desnecessário de informações institucionais;
- c) não instalar programas ou aplicativos não autorizados em equipamentos institucionais;
- d) comunicar imediatamente perda, furto ou roubo de dispositivo pertencente ao IP3P;
- e) evitar utilização de redes ou conexões cuja segurança seja desconhecida;
- f) preservar o sigilo das informações acessadas ou armazenadas.

A PSI disciplina especificamente os dispositivos móveis e atribui ao usuário o dever de comunicar imediatamente eventual furto ou roubo.

10. PROCEDIMENTOS DE CONTINGÊNCIA

Os procedimentos de contingência têm por objetivo assegurar a continuidade, a proteção e, quando necessário, a recuperação das informações e dos recursos tecnológicos utilizados pelo IP3P diante de eventos que possam provocar indisponibilidade, perda, alteração, comprometimento ou acesso indevido às informações institucionais.

Para fins deste Manual, constituem situações que poderão demandar a adoção de procedimentos de contingência, entre outras: falhas em equipamentos ou sistemas, indisponibilidade de serviços informatizados, perda ou corrupção de dados, falhas na execução de cópias de segurança, comprometimento de credenciais, acessos não autorizados, incidentes envolvendo equipamentos ou dispositivos, bem como outras ocorrências capazes de comprometer a confidencialidade, a integridade ou a disponibilidade das informações.

CNPJ: 04.510.687/0001-66

Av. Santos Dumont, nº75 – Bairro Centro – Três Passos/RS – CEP 98600-000





Os procedimentos de contingência compreenderão, no mínimo, a manutenção de cópias de segurança dos sistemas informatizados e bancos de dados, o controle dos acessos físicos e lógicos, a identificação dos responsáveis e as providências necessárias para recuperação ou restabelecimento das informações e serviços afetados.

10.1. Dos Responsáveis

A execução dos procedimentos técnicos de contingência caberá à equipe, empresa contratada ou profissional responsável pela Tecnologia da Informação do IP3P, conforme a estrutura administrativa e os serviços contratados pelo Instituto.

Compete ao responsável pela Tecnologia da Informação, no âmbito de suas atribuições:

- a) executar ou acompanhar as rotinas de cópia de segurança;
- b) verificar a ocorrência de falhas relacionadas aos backups, sistemas, equipamentos ou acessos;
- c) adotar as providências técnicas necessárias ao restabelecimento dos serviços;
- d) realizar, quando necessário, a restauração das informações;
- e) administrar os mecanismos de controle de acesso lógico;
- f) adotar medidas para bloqueio de acessos comprometidos ou desnecessários;
- g) comunicar à Diretoria Executiva as ocorrências relevantes e as providências adotadas.

Compete à Diretoria Executiva acompanhar os procedimentos de contingência, autorizar as providências que extrapolem as atribuições técnicas ordinárias e deliberar sobre medidas administrativas necessárias ao restabelecimento das atividades.

A Política de Segurança da Informação já atribui à equipe de Tecnologia da Informação a administração, proteção e teste das cópias de segurança, a gestão dos acessos e a adoção de medidas de bloqueio quando necessárias.

10.2. Das Cópias de Segurança dos Sistemas e Bancos de Dados

Os sistemas informatizados, bancos de dados, documentos e demais informações digitais essenciais ao funcionamento do IP3P deverão estar abrangidos por procedimentos de cópia de segurança compatíveis com os recursos tecnológicos utilizados pelo Instituto.

As cópias de segurança deverão ser realizadas, preferencialmente, de forma automatizada e em períodos que reduzam o impacto sobre a utilização dos sistemas.

O responsável pela Tecnologia da Informação deverá acompanhar a execução das rotinas de backup, identificando eventuais falhas e adotando as providências necessárias para sua regularização.

Os backups considerados essenciais ao funcionamento das atividades do IP3P deverão observar regras de retenção compatíveis com as necessidades administrativas e com as exigências legais aplicáveis.



12





Sempre que possível, deverá ser mantida cópia adicional em servidor externo ou ambiente em nuvem, como segunda fonte de recuperação das informações.

Na ocorrência de falha na execução do backup ou na restauração das informações, deverá ser realizada nova tentativa tão logo seja identificada e solucionada a causa do problema.

Esses procedimentos correspondem às regras já previstas na PSI do IP3P, que determina a realização preferencialmente automatizada dos backups, o tratamento das falhas e a manutenção das cópias em servidor externo ou nuvem como segunda fonte.

10.3. Do Controle de Acesso Lógico

O acesso aos sistemas informatizados, bancos de dados, redes e demais recursos tecnológicos deverá ser restrito aos usuários devidamente autorizados, de acordo com suas atribuições e necessidades funcionais.

Sempre que tecnicamente possível, cada usuário deverá possuir identificação individual e credencial própria de acesso, sendo vedado o compartilhamento de senhas e credenciais pessoais.

Os acessos deverão ser bloqueados quando deixarem de ser necessários, especialmente em razão de desligamento, exoneração, término da prestação de serviço, alteração de atribuições ou identificação de situação que possa comprometer a segurança das informações.

Quando houver suspeita de comprometimento de senha ou credencial, o acesso deverá ser alterado ou bloqueado, conforme a natureza da ocorrência, até que sejam restabelecidas as condições adequadas de segurança.

As permissões de acesso deverão limitar-se ao necessário para execução das atividades atribuídas ao usuário.

A PSI já determina que os dispositivos de identificação estejam associados a pessoas físicas identificáveis, proíbe o compartilhamento de credenciais e estabelece o bloqueio dos acessos quando deixarem de ser necessários.

10.4. Do Controle de Acesso Físico

O acesso físico aos ambientes, equipamentos e documentos que contenham ou permitam acesso a informações protegidas deverá ser limitado às pessoas autorizadas.

O acesso de visitantes ou terceiros à sala de servidores, quando existente, somente poderá ocorrer acompanhado por servidor próprio ou contratado da área de Tecnologia da Informação ou por servidor expressamente autorizado.

Os documentos físicos que contenham informações de acesso restrito deverão permanecer armazenados em locais adequados, com acesso limitado às pessoas autorizadas.



Quando houver retirada ou consulta de documento físico sujeito a controle, deverá ser realizado o respectivo registro, conforme os procedimentos previstos neste Manual e na Política de Segurança da Informação.

A PSI estabelece tanto o controle de acesso às informações sensíveis mantidas em meio físico quanto a restrição de acesso de visitantes e terceiros à sala de servidores.

10.5. Da Indisponibilidade de Sistemas e Equipamentos

Identificada indisponibilidade de sistema, equipamento, banco de dados, rede ou outro recurso tecnológico necessário às atividades do IP3P, o usuário deverá comunicar a ocorrência ao responsável pela Tecnologia da Informação.

Recebida a comunicação, deverá ser realizada avaliação inicial para identificação da causa e da extensão da indisponibilidade.

Quando possível, serão adotadas medidas para restabelecimento do serviço ou utilização de recurso alternativo disponível.

Caso a indisponibilidade decorra de falha cuja solução dependa de empresa fornecedora do sistema, equipamento ou serviço, deverá ser acionado o respectivo suporte técnico.

As ocorrências que possam causar impacto relevante ou prolongado sobre as atividades do IP3P deverão ser comunicadas à Diretoria Executiva.

10.6. Da Perda ou do Comprometimento de Informações

Na hipótese de perda, exclusão indevida, alteração, corrupção ou suspeita de comprometimento de informações, o usuário que identificar a ocorrência deverá comunicá-la imediatamente ao responsável competente.

O responsável pela Tecnologia da Informação deverá, conforme a natureza da ocorrência:

- a) verificar a extensão do comprometimento;
- b) restringir acessos, quando necessário;
- c) preservar os registros disponíveis relacionados à ocorrência;
- d) verificar a existência de cópia de segurança válida;
- e) realizar ou providenciar a recuperação das informações, quando possível;
- f) comunicar a Diretoria Executiva quando a ocorrência apresentar impacto relevante.

Quando houver indícios de acesso indevido, divulgação não autorizada ou comprometimento de dados pessoais, deverão ser observadas também as normas internas e legais aplicáveis à proteção de dados.





10.7. Da Restauração das Informações

Quando necessária a recuperação de informações a partir das cópias de segurança, a restauração deverá ser executada ou acompanhada pelo responsável pela Tecnologia da Informação.

Antes da restauração, sempre que tecnicamente possível, deverá ser identificada a cópia adequada à recuperação pretendida.

Concluído o procedimento, deverá ser verificada a disponibilidade e integridade das informações restauradas.

Caso a primeira tentativa de restauração não seja bem-sucedida, deverão ser identificadas as causas da falha e adotadas as providências necessárias para nova tentativa.

10.8. Do Registro e Comunicação das Ocorrências

As situações de contingência que apresentem impacto relevante sobre a disponibilidade, integridade ou confidencialidade das informações deverão ser registradas, sempre que aplicável, contendo:

- a) data da ocorrência;
- b) identificação do sistema, equipamento, informação ou recurso afetado;
- c) descrição resumida da ocorrência;
- d) providências adotadas;
- e) responsável pelo atendimento;
- f) resultado das medidas adotadas.

Os registros poderão ser realizados por meio de relatório, chamado técnico, comunicação eletrônica, sistema de atendimento ou outro meio que permita demonstrar a ocorrência e as providências adotadas.

As ocorrências relevantes deverão ser comunicadas à Diretoria Executiva.

10.9. Do Fluxo dos Procedimentos de Contingência

Para fins de padronização, os procedimentos de contingência observarão o seguinte fluxo:

Identificação da ocorrência → Comunicação ao responsável → Avaliação da situação → Adoção das medidas de contenção → Acionamento de backup, suporte ou recurso alternativo, quando necessário → Restabelecimento ou recuperação → Verificação da normalização → Registro da ocorrência → Comunicação à Diretoria Executiva, quando aplicável → Encerramento.

A execução de cada etapa deverá considerar a natureza e a gravidade da ocorrência, não sendo necessária a adoção de medidas que não sejam pertinentes ao evento identificado.





O fluxo deverá ser representado graficamente e mantido juntamente com este Manual, constituindo o **Mapeamento do Procedimento de Contingência do IP3P**.

11. BACKUP E RECUPERAÇÃO DAS INFORMAÇÕES

Os dados e documentos digitais essenciais às atividades do IP3P deverão estar abrangidos por mecanismos de cópia de segurança compatíveis com os recursos tecnológicos disponíveis.

Os backups deverão ser, preferencialmente, automatizados e executados em períodos que reduzam o impacto sobre o funcionamento dos sistemas.

A área responsável deverá acompanhar a execução das rotinas de backup e adotar providências quando identificadas falhas.

Havendo erro na execução ou na restauração, deverá ser realizada nova tentativa tão logo seja solucionada a causa do problema.

Sempre que possível, deverá ser mantida cópia adicional em ambiente externo ou solução em nuvem, reduzindo o risco de perda simultânea das informações.

A Política do IP3P prevê backups automatizados, tratamento de erros e manutenção de cópias em servidor externo ou nuvem como segunda fonte.

12. MONITORAMENTO E AUDITORIA

O IP3P poderá monitorar a utilização dos sistemas, equipamentos, correio eletrônico, internet, rede e demais recursos tecnológicos institucionais, observada a legislação aplicável.

Poderão ser mantidos logs e outros registros destinados a:

- a) identificar acessos;
- b) apurar incidentes;
- c) detectar tentativas de acesso não autorizado;
- d) verificar utilização inadequada dos recursos;
- e) subsidiar auditorias, procedimentos administrativos ou determinações judiciais.

Os registros obtidos deverão ser utilizados exclusivamente para finalidades institucionais legítimas.

A PSI autoriza a implantação de logs, inspeção dos equipamentos institucionais e utilização de mecanismos preventivos e detectivos de segurança.



12





13. GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

Qualquer usuário que identificar situação capaz de comprometer a confidencialidade, integridade ou disponibilidade das informações deverá comunicá-la ao responsável competente.

Podem caracterizar incidentes, entre outras situações:

- a) perda ou furto de equipamento;
- b) suspeita de comprometimento de senha;
- c) acesso não autorizado;
- d) recebimento ou abertura de arquivo malicioso;
- e) perda ou exclusão indevida de informações;
- f) indisponibilidade anormal de sistemas;
- g) divulgação indevida de informações;
- h) identificação de equipamento ou dispositivo desconhecido conectado à rede;
- i) alteração não autorizada de configuração de segurança.

Recebida a comunicação, o responsável deverá avaliar a situação e, conforme o caso:

- a) restringir ou bloquear acessos;
- b) isolar equipamento ou recurso afetado;
- c) alterar credenciais;
- d) preservar registros e evidências disponíveis;
- e) comunicar a Diretoria Executiva;
- f) solicitar suporte técnico especializado;
- g) adotar as providências administrativas, técnicas ou legais pertinentes.

Após a normalização, sempre que a relevância do incidente justificar, deverão ser avaliadas suas causas e as medidas necessárias para reduzir a possibilidade de recorrência.

14. PROTEÇÃO E PRIVACIDADE DAS INFORMAÇÕES

O acesso às informações pessoais e institucionais deverá ocorrer exclusivamente quando necessário ao desempenho das atribuições do usuário.

As informações relativas aos segurados e beneficiários deverão ser tratadas de maneira compatível com sua finalidade e somente disponibilizadas a pessoas autorizadas ou nas hipóteses previstas em lei.

O compartilhamento com empresas contratadas deverá limitar-se às informações necessárias à execução dos serviços e observar as obrigações de confidencialidade e segurança pertinentes.

A PSI determina que as informações sejam acessadas somente por pessoas autorizadas e estabelece critérios para seu fornecimento a terceiros e empresas contratadas.





15. CONSCIENTIZAÇÃO DOS USUÁRIOS

A segurança da informação deverá integrar as ações de orientação e conscientização promovidas pelo IP3P.

Os usuários deverão receber orientação quanto às principais regras de segurança, especialmente em relação:

- a) à proteção das senhas;
- b) à identificação de mensagens e links suspeitos;
- c) ao tratamento adequado de documentos;
- d) ao compartilhamento de informações;
- e) à utilização segura dos equipamentos;
- f) à comunicação de incidentes.

A Política do Instituto estabelece como responsabilidade da área de tecnologia promover a conscientização dos servidores sobre a relevância da segurança da informação.

16. REGISTROS E EVIDÊNCIAS

Os procedimentos de segurança da informação deverão, sempre que aplicável, produzir registros capazes de demonstrar sua execução.

Poderão constituir evidências:

- a) solicitações de criação, alteração e bloqueio de acessos;
- b) protocolos de retirada e devolução de documentos;
- c) registros de backup;
- d) logs de sistemas;
- e) registros de incidentes;
- f) solicitações e registros de manutenção;
- g) termos de ciência e compromisso;
- h) comunicações eletrônicas relacionadas aos procedimentos de segurança;
- i) demais documentos que demonstrem a execução dos controles previstos neste Manual.

Os registros deverão ser mantidos pelo período aplicável, considerando sua finalidade administrativa, legal, previdenciária, fiscal ou de controle.

17. TERMO DE CIÊNCIA E COMPROMISSO

Os servidores, prestadores de serviços e demais usuários sujeitos à Política de Segurança da Informação poderão ser formalmente cientificados de suas responsabilidades mediante assinatura de Termo de Ciência e Compromisso.

O termo deverá registrar, especialmente, o conhecimento das regras de segurança, o compromisso de sigilo e a responsabilidade pela adequada utilização das informações e recursos disponibilizados.

CNPJ: 04.510.687/0001-66

Av. Santos Dumont, nº75 – Bairro Centro – Três Passos/RS – CEP 98600-000





A própria PSI do IP3P contém Termo de Recebimento no qual o signatário declara ciência da política e assume compromisso de preservar a integridade, disponibilidade e confidencialidade das informações mesmo após o encerramento do vínculo.

18. REVISÃO E ATUALIZAÇÃO

Este Manual deverá ser revisto sempre que ocorrerem alterações relevantes na Política de Segurança da Informação, na legislação aplicável, na estrutura administrativa do IP3P, nos sistemas utilizados ou nos procedimentos internos que possam impactar a segurança das informações.

A revisão também poderá decorrer de recomendações de auditoria, identificação de riscos, ocorrência de incidentes ou necessidade de aprimoramento dos controles internos.

As alterações deverão ser formalmente aprovadas pela autoridade competente e divulgadas aos usuários envolvidos.

19. DISPOSIÇÕES FINAIS

O presente Manual de Segurança da Informação estabelece os procedimentos operacionais destinados à implementação das diretrizes previstas na Política de Segurança da Informação do IP3P.

Os procedimentos aqui descritos deverão ser observados por todos os servidores, prestadores de serviços e demais usuários que tenham acesso às informações, sistemas ou recursos tecnológicos do Instituto, conforme suas respectivas atribuições.

Este Manual deverá ser aplicado conjuntamente com a Política de Segurança da Informação e com as demais normas internas do IP3P, não substituindo as obrigações previstas na legislação vigente.

As situações não previstas neste Manual deverão ser submetidas à Diretoria Executiva, com apoio técnico do responsável pela tecnologia da informação quando necessário.

Os procedimentos poderão ser atualizados e aperfeiçoados sempre que identificada necessidade de adequação às práticas administrativas, aos recursos tecnológicos utilizados ou às exigências legais e de governança.

Os casos omissos serão analisados pela Diretoria Executiva, observando-se os princípios da legalidade, eficiência, segurança, transparência, proteção das informações e interesse público.

Elaborado por: IP3P

Aprovado por: Lucas Neckel – Diretor Presidente

Data de aprovação: 08/09/2026



CNPJ: 04.510.687/0001-66

Av. Santos Dumont, nº75 – Bairro Centro – Três Passos/RS – CEP 98600-000



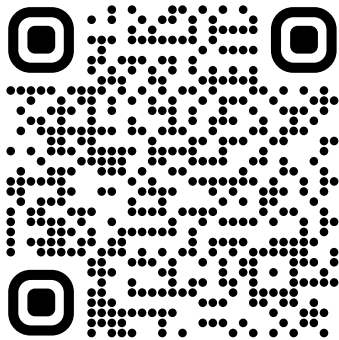
Assinado com Assinatura Eletrônica (Lei 14.063/2020 | Regulamento 910/2014/EC)

Hash SHA256 do original: 8272248c570b5600c2903383d04849a9dd69c07983e2cb73aedfcacf3393b9e9

Link de validação: <https://valida.ae/bb8779dc2c31063abfb49f465810be045a7ca97a3cc456f8f>



Relatório de auditoria e validação de assinaturas eletrônicas



URL pública de verificação de integridade e autenticidade
<https://valida.ae/bb8779dc2c31063abfb49f465810be045a7ca97a3cc456f8f>

Assinaturas concluídas: 1 de 1

Assinaturas eletrônicas realizadas em conformidade com a Lei nº 14.063/2020 e Regulamento (UE) nº 910/2014 (eIDAS)



Como auditar e validar este documento

Você está visualizando uma via para impressão do documento, ela possui os dados de auditoria, porém ela pode ser alterada. Para conferir a integridade do documento e das assinaturas, **acesse a URL pública de validação ou escaneie o QRCode ao lado.**

8272248c570b5600c2903383d04
849a9dd69c07983e2cb73aedfca
cf3393b9e9 Hash SHA256 do original

Assinaturas presentes no documento



Lucas Neckel
Assinado eletronicamente por
Lucas Neckel
Data: 08/09/2026 09:38
#3c344724ab8211f1818d42010a2b6021

SIGNATÁRIO

Trilha de auditoria

08/09/2026 09:38 Lucas Neckel (lucas.ip3p@trespassos.rs.gov.br, CPF 982.436.240-15) criou o documento

Hash SHA256 do arquivo: 8272248c570b5600c2903383d04849a9dd69c07983e2cb73aedfcafcf3393b9e9

08/09/2026 09:38 Lucas Neckel (lucas.ip3p@trespassos.rs.gov.br, CPF 982.436.240-15) visualizou o documento

Endereço de IP: 138.219.252.216 Porta: 58533

08/09/2026 09:38 Lucas Neckel (lucas.ip3p@trespassos.rs.gov.br, CPF 982.436.240-15) assinou o documento

Endereço de IP: 138.219.252.216 Navegador: Chrome/152.0.0.0 Tipo de geolocalização: IP
Porta: 58533 Arquitetura: x64 Precisão: 5km+
SO: Windows 10.0 Render engine: Gecko Latitude e longitude: -27.4348, -53.9224