POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DA RIOPRETOPREV

Versão 4.0, de 27 de agosto de 2026

Resumo

A Política da Segurança da Informação - PSI - é uma declaração formal de compromisso da RIOPRETOPREV com a proteção das informações sob sua guarda. Documento aprovado na 14ª Reunião da Comissão de Segurança da Informação/CSI – Realizada em 27/08/2026. Documento elaborado em atendimento ao disposto no item 3.1.5 do Manual do Pró-Gestão RPPS.

Comissão de Segurança da Informação – CSI/RPP

contato@riorpetoprev.sp.gov.br

Regime Próprio de Previdência Social do Município de São José do Rio Preto - RIOPRETOPREV

Cel. Fábio Rogério Candido
Prefeito Municipal

Cel. Miguel Elias Daffara
Diretor Superintendente

Wilclem de Lazari Araújo
Diretor Técnico

Adriano Antônio Pazianoto
Diretor Executivo

Comissão de Segurança da Informação – CSI/RPP
Adriano Antônio Pazianoto
Fabiano Hernandes de Assis
Ludmila Andrade Sernagiotto de Souza
Mário José Piccarelli de Castro

RIOPRETOPREV – Regime Próprio de Previdência Social do Município de São José do Rio Preto
Rua General Glicério, 3553 – Centro - CEP 15015-400 - São José do Rio Preto - SP Telefones (17) 3222 7445
E-mail: contato@riopretoprev.sp.gov.br - www.riopretoprev.sp.gov.br

Controle de versão

Identificação do documento	Descrição
Título	Política de Segurança da Informação (PSI) da RIOPRETOPREV
Versão	4.0
Data da versão	27/08/2026
Elaboração	Comissão de Segurança da Informação (CSI/RPP)
Aprovação	Comissão de Segurança da Informação (CSI/RPP), com homologação da Diretoria Executiva
Ato de aprovação	Ata da CSI/RPP
Vigência	Documento em elaboração. A vigência inicia-se na data de publicação, após a aprovação pelo CSI/RPP, substituindo integralmente a versão anterior
Periodicidade de revisão	Revisão ordinária no mínimo a cada 4 (quatro) anos, com avaliação anual de aderência e revisão extraordinária nas hipóteses previstas nas Considerações finais
Classificação da informação	Pública
Publicação	Sítio eletrônico da RIOPRETOPREV (www.riopretoprev.sp.gov.br) e intranet da Autarquia
Responsável pela guarda e pelo controle de versões	Comissão de Segurança da Informação (CSI/RPP)

Histórico de revisões

Versão	Data	Descrição das alterações	Elaboração	Aprovação
1.0	2018	Versão inicial da Política de Segurança da Informação da RIOPRETOPREV, elaborada em atendimento ao item 3.1.5 do Manual do Pró-Gestão RPPS. Estabeleceu a estrutura original do documento, mantida nas versões seguintes, com dezesseis seções: introdução, objetivos, princípios, responsabilidades, correio eletrônico, comunicador instantâneo, internet e VPN, servidor de arquivos, identificação pessoal, equipamentos, comportamento esperado, dispositivos móveis, backup, assinatura e processo digital, arquivos digitalizados e considerações finais.	-	-
2.0	2020	Atualização da Política, com manutenção da estrutura de dezesseis seções e publicação no sítio eletrônico da Autarquia. Adotava o Spark como comunicador instantâneo oficial, admitida a utilização de outras ferramentas equivalentes, e disciplinava o servidor de arquivos provido pela Empro como repositório institucional. Vinculou a digitalização de documentos ao Decreto Federal nº 10.278/2020, remetendo a Portaria específica a publicação do Código de Classificação e da Tabela de Temporalidade.	-	-
3.0	18/09/2023	Inclusão da seção "Da Política de Privacidade de Dados Pessoais", com a previsão de edição de documento específico sobre coleta, uso, proteção e direitos dos	CSI/RPP	CSI/RPP

RIOPRETOPREV – Regime Próprio de Previdência Social do Município de São José do Rio Preto
Rua General Glicério, 3553 – Centro - CEP 15015-400 - São José do Rio Preto - SP Telefones (17) 3222 7445
E-mail: contato@riopretoprev.sp.gov.br - www.riopretoprev.sp.gov.br

		titulares. Identificação da Comissão de Segurança da Informação (CSI/RPP) como responsável pelo documento e vinculação expressa ao item 3.1.5 do Manual do Pró-Gestão RPPS. Estabelecimento de revisão bienal. Aprovada na 1ª Reunião Extraordinária do CSI/RPP.		
3.1	18/12/2023	Inclusão das seções "Auditoria de Acesso" e "Recuperação de Desastres", com a definição de políticas de acesso, revisão de permissões, monitoramento, registro de auditoria, testes de penetração, treinamento de usuários, análise de riscos, procedimentos e testes de recuperação, pessoal-chave, comunicação de emergência e atualização contínua. Reescrita integral da seção "Backup (cópia de segurança)", com a descrição das rotinas automáticas mantidas pelos fornecedores dos sistemas. Aprovada na 1ª Reunião Extraordinária do CSI/RPP.	CSI/RPP	CSI/RPP
4.0	27/08/2026	Revisão geral para atendimento ao Nível IV da ação 3.1.5 do Manual do Pró-Gestão RPPS, versão 4.1. Substituição do comunicador Spark pelo Microsoft Teams, com adoção do ambiente Microsoft 365, e formalização do canal corporativo de atendimento por WhatsApp, com vedação do uso de contas pessoais de aplicativos de mensagem. Inclusão das seções Resumo Executivo, Controle de Versão, Gestão da Segurança da Informação, Classificação da Informação, Uso de Inteligência Artificial, Resposta a Incidentes de Segurança da Informação, Proteção de Endpoint e Antivírus, Controle de Acesso Físico, Inventário de Ativos de Informação, Gestão de Riscos de Segurança da Informação, Gestão de Fornecedores e Terceiros, Termo de Responsabilidade e Referências Normativas. Complementação da política de senhas, com tamanho mínimo, bloqueio por tentativas malsucedidas, vedação de reuso, periodicidade de troca, senha provisória no primeiro acesso, regras de guarda e tratamento das contas privilegiadas e genéricas. Definição do conteúdo mínimo dos registros de auditoria, da sincronização de relógio e dos prazos objetivos de retenção de logs por categoria, com vedação de exclusão antecipada e preservação em caso de apuração em curso. Inclusão da autenticação multifator, da regra de revogação imediata de acesso lógico e físico e das rotinas de teste de restauração com metas de RTO e RPO. Harmonização das regras de armazenamento nos repositórios institucionais e substituição do limite fixo de anexo de correio eletrônico pelo limite da plataforma institucional. Designação do	CSI/RPP	CSI/RPP

RIOPRETOPREV – Regime Próprio de Previdência Social do Município de São José do Rio Preto
Rua General Glicério, 3553 – Centro - CEP 15015-400 - São José do Rio Preto - SP Telefones (17) 3222 7445
E-mail: contato@riopretoprev.sp.gov.br - www.riopretoprev.sp.gov.br

		Encarregado de Dados, manutenção do ROPA e fixação dos prazos de comunicação e de guarda de incidentes, nos termos da Resolução CD/ANPD nº 15/2024. Remissão expressa aos manuais internos de procedimento vigentes, com indicação de título, versão e data, e ao Código de Classificação e à Tabela de Temporalidade aprovados pela Portaria nº 385/2020. Alteração do prazo de revisão ordinária de 2 (dois) para 4 (quatro) anos, com avaliação anual de aderência, e inclusão do Anexo I com a matriz de atendimento ao Manual do Pró-Gestão RPPS.		

RIOPRETOPREV – Regime Próprio de Previdência Social do Município de São José do Rio Preto
Rua General Glicério, 3553 – Centro - CEP 15015-400 - São José do Rio Preto - SP Telefones (17) 3222 7445
E-mail: contato@riopretoprev.sp.gov.br - www.riopretoprev.sp.gov.br

Resumo Executivo

Esta Política de Segurança da Informação consolida as diretrizes institucionais da RIOPRETOPREV para proteção das informações sob sua guarda, abrangendo confidencialidade, integridade, disponibilidade, rastreabilidade, controle de acessos, classificação da informação, tratamento de incidentes, proteção de dados pessoais, uso de inteligência artificial, gestão de fornecedores, backup, recuperação de desastres e responsabilidades dos usuários internos e externos.

O documento foi estruturado para atender às exigências de governança, controles internos e segurança da informação aplicáveis aos Regimes Próprios de Previdência Social, com especial atenção ao Manual do Pró-Gestão RPPS, versão 4.1, vigente em 2026, especialmente ao item 3.1.5 - Política de Segurança da Informação, Nível IV, e às normas correlatas de proteção de dados, acesso à informação, gestão documental e boas práticas de segurança da informação.

Em termos práticos, a Política define condutas obrigatórias e vedadas, estabelece responsabilidades para colaboradores, gestores, visitantes e fornecedores, disciplina o uso de recursos tecnológicos, orienta a classificação e o tratamento das informações, formaliza procedimentos de resposta a incidentes e cria bases documentais para auditoria, revisão periódica e melhoria contínua. Também reforça a atuação da Comissão de Segurança da Informação da RIOPRETOPREV como instância de acompanhamento, orientação e controle.

A matriz de atendimento constante do Anexo I demonstra a correlação entre os requisitos do Manual do Pró-Gestão RPPS, versão 4.1, para o Nível IV da ação 3.1.5 - Política de Segurança da Informação, e os dispositivos constantes desta Política, permitindo evidenciar, de forma objetiva, os pontos de conformidade já contemplados e os elementos de controle que deverão ser mantidos atualizados para fins de certificação, auditoria e supervisão.

RIOPRETOPREV – Regime Próprio de Previdência Social do Município de São José do Rio Preto
Rua General Glicério, 3553 – Centro - CEP 15015-400 - São José do Rio Preto - SP Telefones (17) 3222 7445
E-mail: contato@riopretoprev.sp.gov.br - www.riopretoprev.sp.gov.br

Sumário

Controle de versão 2
Histórico de revisões 2
Resumo Executivo 5
Sumário 6
Introdução 7
Objetivos 7
Princípios 8
Responsabilidades 9
Colaboradores 9
Visitantes 9
Gestores 9
Pessoas jurídicas contratadas 9
Clientes 9
Correio eletrônico 10
Comunicador instantâneo 10
WhatsApp corporativo (canal oficial de atendimento) 11
Internet e VPN 12
Servidor de arquivos 13
Identificação pessoal 13
Equipamentos 15
Comportamento esperado (boas práticas) 15
Gestão da Segurança da Informação 16
Dispositivos móveis 16
Backup (cópia de segurança) 16
Auditoria de Acesso 17
Recuperação de Desastres 19
Assinatura e processo digital 20
Classificação da Informação 21
Arquivos digitalizados 21
Da Política de Privacidade de Dados Pessoais 21
Uso de Inteligência Artificial 22
Resposta a Incidentes de Segurança da Informação 24
Proteção de Endpoint e Antivírus 24
Controle de Acesso Físico 24
Inventário de Ativos de Informação 25
Gestão de Riscos de Segurança da Informação 25
Gestão de Fornecedores e Terceiros 25
Termo de Responsabilidade 26
Referências Normativas 26
Considerações finais 27
Anexo I - Matriz de atendimento ao Manual do Pró-Gestão RPPS, versão 4.1, Nível IV 27

RIOPRETOPREV – Regime Próprio de Previdência Social do Município de São José do Rio Preto
Rua General Glicério, 3553 – Centro - CEP 15015-400 - São José do Rio Preto - SP Telefones (17) 3222 7445
E-mail: contato@riopretoprev.sp.gov.br - www.riopretoprev.sp.gov.br

Introdução

Este documento estabelece as diretrizes corporativas de segurança da informação aplicáveis às informações produzidas, recebidas, manipuladas, armazenadas e transmitidas pela RIOPRETOPREV.

A Política de Segurança da Informação (PSI) tem o intuito de garantir, principalmente, que as informações sejam protegidas, tanto no que se refere à confidencialidade quanto à integridade dos dados, bem como que estejam sempre disponíveis a quem delas necessita e a quem é de direito.

Sempre que uma informação é manipulada, ela está sujeita a erros decorrentes de falhas humanas, falhas técnicas ou do uso inadequado dos sistemas. Por isso, é necessário estabelecer diretrizes que reduzam esse risco e protejam a informação corporativa.

Este documento está publicado no sítio eletrônico da RIOPRETOPREV na Internet (www.riopretoprev.sp.gov.br), aberto para consultas, e disponível também na intranet da Autarquia.

Objetivos

Esta Política tem por objetivo orientar os servidores da RIOPRETOPREV e demais interessados quanto aos procedimentos necessários para reforçar a segurança dos dados e das informações institucionais.

A ideia é alertar os membros da autarquia quanto às possíveis consequências dos seus atos e o que deve ser feito para melhor tratar as informações de sua competência. Com relação aos interessados externos, o documento informa como as informações do órgão podem ser acessadas.

São definidas aqui as responsabilidades e as boas práticas, separadas por assuntos.

RIOPRETOPREV – Regime Próprio de Previdência Social do Município de São José do Rio Preto
Rua General Glicério, 3553 – Centro - CEP 15015-400 - São José do Rio Preto - SP Telefones (17) 3222 7445
E-mail: contato@riopretoprev.sp.gov.br - www.riopretoprev.sp.gov.br

Princípios

Toda informação produzida ou recebida pelos colaboradores como resultado da atividade profissional pertence à instituição. As exceções devem ser explícitas e formalizadas.

Os equipamentos de informática e comunicação, os sistemas e as informações são disponibilizados aos colaboradores para a realização de atividades profissionais. O uso pessoal dos recursos é permitido desde que não prejudique o desempenho dos sistemas e serviços e esteja plenamente de acordo com o Código de Ética da instituição.

Qualquer incidente ou suspeita de incidente que possa afetar a segurança da informação deverá ser comunicado imediatamente à Comissão de Segurança da Informação (CSI/RPP) e ao Encarregado de Dados (DPO) da RIOPRETOPREV, por meio dos canais oficiais (e-mail institucional do CSI/RPP ou registro no sistema de processo digital), para que as devidas providências de contenção, investigação e comunicação sejam adotadas, inclusive, quando cabível, à Autoridade Nacional de Proteção de Dados (ANPD), nos termos da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018).

RIOPRETOPREV – Regime Próprio de Previdência Social do Município de São José do Rio Preto
Rua General Glicério, 3553 – Centro - CEP 15015-400 - São José do Rio Preto - SP Telefones (17) 3222 7445
E-mail: contato@riopretoprev.sp.gov.br - www.riopretoprev.sp.gov.br

Responsabilidades

Colaboradores

É considerado colaborador qualquer pessoa que tenha vínculo empregatício de tempo indeterminado com a autarquia; podem ser funcionários estatutários ou sob outro regime jurídico, incluindo estagiários.

Tais pessoas têm responsabilidade sobre todas as informações de que têm conhecimento e/ou que manipulam em razão do seu serviço, devendo zelar por sua proteção.

Visitantes

Qualquer pessoa que venha até a sede da autarquia é considerada visitante. Estará sujeita à PSI, devendo zelar pelas informações da RIOPRETOPREV que tem conhecimento em razão do seu trabalho, bem como qualquer eventual uso de equipamento ou infraestrutura.

O visitante deve sempre ser supervisionado pela pessoa visitada, a qual é responsável pelos dados aos quais o primeiro tem acesso e pelos equipamentos utilizados. Além disso, o visitado tem a responsabilidade de avisar ao visitante sobre as normas de PSI da RIOPRETOPREV.

Os prestadores de serviço também são caracterizados como visitantes.

Gestores

Qualquer pessoa que possua colaborador, equipe ou processo sob sua supervisão é considerada gestora. Além de responder por seus próprios atos, também responde pelos atos de seus subordinados diretos, devendo zelar pela proteção das informações manipuladas por sua equipe.

O gestor deve ser o modelo de conduta na equipe, orientando-a e fiscalizando-a para que incidentes relacionados à PSI não ocorram. Ele também deverá adaptar os processos e procedimentos de sua responsabilidade à política, cuidando para que ela não seja infringida.

Pessoas jurídicas contratadas

Qualquer pessoa jurídica que seja ou venha a ser contratada para prestação de serviços à RIOPRETOPREV é responsável por cuidar das informações da autarquia de que tiver conhecimento, seja mediante contrato ou solicitação de serviço. As pessoas jurídicas também são responsáveis pelos prestadores de serviços enviados, respondendo solidariamente por qualquer incidente ocorrido com eles.

A pessoa jurídica que possuir banco de dados com informações de propriedade da RIOPRETOPREV deve zelar pela sua proteção, em termos de confidencialidade, integridade ou disponibilidade dos dados. Deve estar claro que todos os dados pertencem à autarquia.

A premissa apresentada no parágrafo anterior se estende aos equipamentos que porventura sejam submetidos a manutenção e à pessoa jurídica responsável por tal serviço.

Os dados fornecidos pela RIOPRETOPREV à pessoa jurídica contratada não devem ser divulgados ou repassados a terceiros sem que haja autorização explícita.

Clientes

São considerados clientes da RIOPRETOPREV todos os segurados e beneficiários do regime que necessitam de qualquer serviço prestado pela Autarquia.

A responsabilidade sobre as informações a que o cliente tem direito, ou passa a conhecer, é do colaborador que realizou o contato e do gestor imediato do departamento ao qual o ato ocorreu.

RIOPRETOPREV – Regime Próprio de Previdência Social do Município de São José do Rio Preto
Rua General Glicério, 3553 – Centro - CEP 15015-400 - São José do Rio Preto - SP Telefones (17) 3222 7445
E-mail: contato@riopretoprev.sp.gov.br - www.riopretoprev.sp.gov.br

Correio eletrônico

O uso do correio eletrônico da RIOPRETOPREV é para fins corporativos e relacionados às atividades do colaborador usuário. A utilização desse serviço para fins pessoais é permitida desde que seja feita com bom senso e sem conflito com qualquer norma do Código de Ética, não prejudique a autarquia e nem cause impacto no tráfego da rede.

É vedado aos colaboradores da RIOPRETOPREV:

- Enviar mensagens não solicitadas para múltiplos destinatários, exceto se relacionadas a uso legítimo da instituição e com ciência da Gerência de Cadastro e Sistemas de Informação, área responsável pela Tecnologia da Informação na RIOPRETOPREV;
- Enviar mensagens usando nome de usuário de outra pessoa ou endereço eletrônico que não esteja autorizado a usar;
- Enviar qualquer e-mail que torne seu remetente e/ou a RIOPRETOPREV vulneráveis a ações civis ou criminais;
- Divulgar externamente informações não autorizadas ou imagens de tela, sistemas, documentos e afins sem autorização explícita;
- Falsificar ou adulterar informações do cabeçalho do e-mail;
- Produzir, transmitir ou divulgar mensagem que:
    - Conflite com os interesses da autarquia;
    - Contenha ameaças eletrônicas, como spam ou vírus;
    - Vise obter acesso não autorizado a outro computador ou servidor;
    - Vise interromper um serviço por meio de método ilícito;
    - Vise burlar qualquer sistema de segurança;
    - Vise vigiar secretamente ou assediar outro usuário;
    - Vise acessar informações confidenciais sem autorização explícita do proprietário;
    - Possua anexo que exceda o limite de tamanho estabelecido pela plataforma de correio eletrônico institucional, devendo o envio de arquivos volumosos ser realizado por meio de link de compartilhamento do OneDrive ou do SharePoint, com permissão restrita aos destinatários;
    - Tenha conteúdo considerado impróprio, obsceno ou ilegal;
    - Seja caluniosa, difamatória ou ofensiva;
    - Tenha fins políticos (propaganda);
    - Inclua material protegido por direitos autorais sem a permissão do detentor.

Toda mensagem enviada pelo correio eletrônico deve possuir uma assinatura que identifique claramente o remetente.

O colaborador deve estar atento a mensagens de correio eletrônico que apresentem características de *phishing* ou engenharia social, tais como: remetentes desconhecidos ou com endereços similares aos oficiais, solicitações urgentes de dados pessoais ou senhas, links suspeitos e anexos não solicitados. Caso receba mensagens com tais características, o colaborador não deverá clicar em links, abrir anexos ou fornecer qualquer informação, devendo encaminhar imediatamente a mensagem suspeita ao CSI/RPP e excluí-la da caixa de entrada. É obrigatório o uso do campo 'Cópia Oculta' (CCO/BCC) para envios coletivos a destinatários externos ou que não necessitem visualizar os demais endereços.

Comunicador instantâneo

O comunicador instantâneo oficial da RIOPRETOPREV para comunicação interna é o Microsoft Teams, integrante do pacote Microsoft 365 adotado pela Autarquia. O Microsoft Teams é a ferramenta oficial para chat interno, videoconferência, mensagens instantâneas, reuniões e compartilhamento de arquivos no âmbito do CSI/RPP e de toda a instituição, conforme art. 21 do Regimento Interno do CSI/RPP. Para a

RIOPRETOPREV – Regime Próprio de Previdência Social do Município de São José do Rio Preto
Rua General Glicério, 3553 – Centro - CEP 15015-400 - São José do Rio Preto - SP Telefones (17) 3222 7445
E-mail: contato@riopretoprev.sp.gov.br - www.riopretoprev.sp.gov.br

comunicação com segurados, beneficiários e demais interessados externos, aplica-se o disposto na subseção "WhatsApp corporativo (canal oficial de atendimento)".

São vedados os seguintes comportamentos nos comunicadores instantâneos a serviço da RIOPRETOPREV:

- Divulgar externamente informações não autorizadas ou imagens de tela, sistemas, documentos e afins sem autorização explícita;
- Enviar mensagens passando-se por outro usuário;
- Utilizar conta alheia sem autorização explícita e sem identificar-se adequadamente;
- Enviar mensagens difamatórias, ofensivas, preconceituosas, obscenas, caluniosas ou com fins de propaganda política;
- Utilizar avatares, fotos de perfil ou status que sejam difamatórios, ofensivos, preconceituosos, obscenos, caluniosos ou com fins de propaganda política.

Caso haja a necessidade de realização de videoconferência com compartilhamento de tela, o usuário responsável deve garantir que nenhuma informação além da estritamente necessária seja transmitida. O conteúdo textual das comunicações realizadas via Microsoft Teams é armazenado em nuvem conforme as políticas de retenção definidas pela Autarquia, podendo ser consultado para fins de auditoria e conformidade.

WhatsApp corporativo (canal oficial de atendimento)

A RIOPRETOPREV mantém canal corporativo de atendimento por WhatsApp, vinculado a conta oficial verificada junto à Meta e operado exclusivamente por meio de plataforma de atendimento homologada, baseada na WhatsApp Business API (WABA). Esse canal constitui o meio prioritário de comunicação oficial com segurados, beneficiários, pensionistas e demais interessados externos, ressalvadas as hipóteses em que a legislação, o ato normativo ou o próprio procedimento exigir forma específica, tais como publicação oficial, autuação em processo digital, correio eletrônico institucional ou atendimento presencial.

No uso do canal corporativo de WhatsApp devem ser observadas as seguintes regras:

- O atendimento é realizado somente por servidores previamente autorizados, mediante credenciais pessoais e intransferíveis de acesso à plataforma, com registro do responsável por cada interação;
- É vedado utilizar número ou conta pessoal para atendimento institucional, bem como transferir a tratativa para conta não corporativa;
- É vedado solicitar senhas, códigos de verificação ou dados de acesso do interessado por esse canal;
- A identidade do interessado deve ser confirmada antes da transmissão de informações restritas ou sigilosas, limitando-se o conteúdo enviado ao estritamente necessário à finalidade do atendimento;
- Requerimentos, documentos comprobatórios e decisões que produzam efeitos administrativos devem ser autuados e tramitados no sistema de processo digital, cabendo ao canal a função de contato, orientação e encaminhamento;
- Aplicam-se ao canal, no que couber, as vedações previstas nesta seção quanto ao conteúdo das mensagens e ao uso de imagens de perfil.

Os registros das interações mantidos na plataforma de atendimento observam os prazos de guarda do Código de Classificação e da Tabela de Temporalidade e Destinação de Documentos da RIOPRETOPREV, aprovados pela Portaria nº 385/2020, e podem ser consultados para fins de auditoria e conformidade. O fornecedor da plataforma é tratado como operador, submetendo-se às exigências da seção "Gestão de Fornecedores e Terceiros", e a operação de tratamento correspondente deve constar do Registro das Operações de Tratamento de Dados Pessoais (ROPA) e da Política de Privacidade da Autarquia.

Ressalvado o canal corporativo de que trata esta subseção, é vedado o uso de contas pessoais de WhatsApp, Telegram e aplicativos similares para tratar de assuntos institucionais, transmitir documentos ou compartilhar dados pessoais de segurados, beneficiários e servidores. Na hipótese de o contato ser iniciado por terceiros em conta pessoal, o servidor deverá redirecionar a tratativa para o canal corporativo de atendimento, para o Microsoft Teams ou para o sistema de processo digital, conforme o caso, e nele registrar o conteúdo relevante.

RIOPRETOPREV – Regime Próprio de Previdência Social do Município de São José do Rio Preto
Rua General Glicério, 3553 – Centro - CEP 15015-400 - São José do Rio Preto - SP Telefones (17) 3222 7445
E-mail: contato@riopretoprev.sp.gov.br - www.riopretoprev.sp.gov.br

Internet e VPN

Embora a conexão direta e permanente da rede corporativa com a internet ofereça grande potencial de benefícios, ela abre a porta para riscos significativos para os ativos da informação. Todas as regras estabelecidas pela empresa contratada para provimento da internet e administração da rede devem ser seguidas.

Qualquer informação que é acessada, transmitida, recebida ou produzida na internet está sujeita a divulgação e auditoria. Portanto, a RIOPRETOPREV, em total conformidade legal, reserva-se o direito de solicitar o monitoramento e o registro de todos os acessos a ela.

A internet disponibilizada pode ser usada com finalidade pessoal, desde que não prejudique a produtividade da unidade e não onere a rede, causando lentidão ou outros problemas. Da mesma forma, seu uso não deve ferir qualquer norma do Código de Ética vigente.

É proibida a divulgação de qualquer informação corporativa em redes sociais, listas de discussão, comunidades de relacionamento ou a terceiros via comunicadores eletrônicos ou qualquer outra tecnologia que venha surgir da internet, salvo quando realizado pelas pessoas autorizadas a realizar comunicação externa.

É proibido o *download* e a instalação de softwares que tenham direitos autorais, marca registrada ou patente na internet e que não foram devidamente adquiridos pela autarquia. Isso se aplica também ao download de mídias e arquivos em geral que não sejam de uso livre, sejam eles imagens, apresentações, planilhas, músicas, entre outros. É proibido expor, armazenar, distribuir, editar, imprimir ou gravar materiais de cunho sexual, obsceno, difamatório, ofensivo, preconceituoso e político (propaganda) por qualquer meio.

É permitido aos colaboradores usarem a conexão Wi-Fi disponibilizada pela Empro, desde que em conformidade com as normas do Código de Ética e mediante o devido cadastro junto à empresa.

Para o trabalho à distância, é disponibilizado a cada servidor acesso remoto à rede interna e, consequentemente, aos dados necessários e ao computador de trabalho mediante VPN (*Virtual Private Network*).

Uma vez conectado à VPN, o servidor está sujeito às mesmas regras do que quando utilizando a rede interna da RIOPRETOPREV no local de trabalho, já que a tecnologia habilita que o usuário possa trabalhar remotamente da mesma forma que trabalharia *in loco*.

Tanto a senha utilizada para conexão quanto o arquivo de configuração da rede VPN são individuais e intransferíveis, devendo o portador zelar pela confidencialidade dessas informações, visto que a principal função de uma VPN é estabelecer uma conexão segura entre um computador que esteja fora da rede corporativa com um ou mais computadores dentro da rede corporativa.

Como a VPN pode permitir a transferência de arquivos entre redes distintas, devem ser observadas as regras da seção "Dispositivos móveis", com a adoção das cautelas necessárias para impedir que informações utilizadas no trabalho sejam acessadas por pessoa não autorizada no equipamento do usuário. Assim, recomenda-se que a transferência de arquivos seja realizada apenas quando imprescindível à atividade profissional.

O acesso remoto à rede corporativa da RIOPRETOPREV, seja por VPN ou por qualquer outra tecnologia de acesso remoto (incluindo acesso aos serviços em nuvem do Microsoft 365), deverá obrigatoriamente utilizar autenticação multifator (MFA — Multi-Factor Authentication), quando disponível, combinando a senha pessoal com um segundo fator de verificação (aplicativo autenticador, SMS ou token físico).

No trabalho remoto ou híbrido, o servidor deve observar, adicionalmente, as seguintes regras:

- Utilizar exclusivamente equipamentos autorizados pela Autarquia ou, na impossibilidade, garantir que o dispositivo pessoal possua antivírus atualizado e sistema operacional com as últimas atualizações de segurança;
- Não utilizar redes Wi-Fi públicas ou abertas para acessar sistemas ou dados da RIOPRETOPREV, salvo se conectado à VPN institucional;
- Ao término da sessão de trabalho remoto, realizar o logoff de todos os sistemas e desconectar a VPN;

RIOPRETOPREV – Regime Próprio de Previdência Social do Município de São José do Rio Preto
Rua General Glicério, 3553 – Centro - CEP 15015-400 - São José do Rio Preto - SP Telefones (17) 3222 7445
E-mail: contato@riopretoprev.sp.gov.br - www.riopretoprev.sp.gov.br

- Não armazenar arquivos institucionais no disco local do equipamento, utilizando exclusivamente os repositórios institucionais definidos na seção "Servidor de arquivos".

Servidor de arquivos

São repositórios institucionais autorizados para o armazenamento de arquivos de trabalho da RIOPRETOPREV o ambiente em nuvem do Microsoft 365 (OneDrive e SharePoint), de uso preferencial, e o servidor de arquivos de rede provido pela Empro. Ambos estão submetidos a rotinas de cópia de segurança e a controle de permissões. É vedado o armazenamento de arquivos institucionais exclusivamente no disco local de estações de trabalho, bem como em equipamentos, mídias ou serviços pessoais.

O uso deste servidor de arquivos (provido pela Empro) é permitido a todos os usuários. Entretanto, os diretórios existentes ali estão permissionados de acordo com o organograma vigente na instituição.

Caso haja alguma necessidade de alteração no permissionamento, esta deverá ser comunicada e justificada à Gerência de Cadastro e Sistemas de Informação para avaliação e concessão, caso seja aplicável.

Além dos diretórios correspondentes às coordenadorias e grupos, existem os diretórios de compartilhamentos, nos quais os usuários podem compartilhar arquivos com outros, entre coordenadorias iguais ou distintas.

Não é permitido armazenar arquivos que não tenham relação com o trabalho realizado, especialmente filmes e músicas, mesmo que isto aparentemente não cause prejuízo à instituição.

É vedado:

- Armazenar vídeos e músicas;
- Armazenar conteúdo difamatório, ofensivo, preconceituoso, obsceno, sexual, calunioso ou que tenha fins de propaganda política;
- Editar ou apagar arquivos de outros usuários sem autorização destes;
- Fraudar, de qualquer forma, as informações dos arquivos;
- Instalar ou armazenar programas sem o conhecimento da Gerência de Cadastro e Sistemas de Informação;
- Armazenar conteúdo nocivo, como vírus e *malwares*;
- Armazenar conteúdo protegido por direitos autorais ou patentes.

Qualquer necessidade de armazenamento de arquivo que se configure como exceção às regras apresentadas deve ser comunicada à Gerência de Cadastro e Sistemas de Informação para avaliação, desde que haja justificativa plausível.

Identificação pessoal

Os dispositivos de identificação, incluindo CPF, assinadores digitais e senhas, protegem a identidade do colaborador usuário, prevenindo que uma pessoa se faça passar por outra perante a RIOPRETOPREV ou terceiros.

O uso dos dispositivos e/ou senhas de identificação de outra pessoa constitui crime tipificado no Código Penal Brasileiro (art. 307 – falsa identidade).

Tal norma visa estabelecer critérios de responsabilidade sobre o uso dos dispositivos de identificação e deverá ser aplicada a todos os colaboradores. O usuário, vinculado a tais dispositivos identificadores, será responsável pelo seu uso correto perante a instituição e a legislação (cível e criminal).

As senhas utilizadas para o acesso aos equipamentos e serviços são de uso pessoal e intransferível, não devendo ser armazenadas em arquivos eletrônicos compreensíveis por linguagem humana (sem criptografia), bem como baseadas em informações pessoais e padrões óbvios, como "12345", "654321", "qwert", entre outros.

As senhas de acesso aos sistemas, equipamentos e serviços da RIOPRETOPREV devem observar os parâmetros mínimos a seguir, que serão implementados por configuração dos próprios sistemas sempre que a solução permitir e, quando não houver esse recurso, exigidos do usuário no momento da criação da senha:

RIOPRETOPREV – Regime Próprio de Previdência Social do Município de São José do Rio Preto
Rua General Glicério, 3553 – Centro - CEP 15015-400 - São José do Rio Preto - SP Telefones (17) 3222 7445
E-mail: contato@riopretoprev.sp.gov.br - www.riopretoprev.sp.gov.br

- Possuir, no mínimo, 10 (dez) caracteres, elevados a 14 (quatorze) caracteres nas contas com privilégios administrativos ou de superusuário;
- Utilizar ao menos um dígito;
- Utilizar ao menos uma letra minúscula;
- Utilizar ao menos uma letra maiúscula;
- Utilizar ao menos um símbolo especial, como '@', '#', '$' entre outros;
- Não conter o nome do usuário, sua matrícula, seu CPF, datas comemorativas, nomes de familiares, o nome da Autarquia ou sequências previsíveis de teclado.

A conta será bloqueada automaticamente após 5 (cinco) tentativas malsucedidas consecutivas de autenticação, permanecendo indisponível por, no mínimo, 30 (trinta) minutos ou até o desbloqueio pela Gerência de Cadastro e Sistemas de Informação. As tentativas malsucedidas são registradas e compõem o monitoramento previsto na seção "Auditoria de Acesso".

É vedada a reutilização das 5 (cinco) últimas senhas empregadas pelo usuário, bem como a alteração meramente formal por acréscimo ou substituição de um único caractere em relação à senha anterior.

A troca periódica de senha será exigida a cada 12 (doze) meses nas contas de usuário comum e a cada 6 (seis) meses nas contas com privilégios administrativos. Independentemente da periodicidade, a troca imediata é obrigatória sempre que houver suspeita de comprometimento, comunicação de incidente, uso indevido de credenciais ou determinação do CSI/RPP. Nos sistemas que exijam autenticação multifator (MFA), a periodicidade poderá ser dispensada mediante deliberação do CSI/RPP registrada em ata, hipótese em que permanecem exigíveis os demais parâmetros desta seção.

A senha fornecida no momento da criação da credencial é provisória e deve ser alterada pelo usuário no primeiro acesso. As senhas padrão de fábrica de equipamentos, sistemas e dispositivos de rede devem ser substituídas antes da entrada em operação.

É vedado compartilhar senhas com terceiros, inclusive com colegas, chefias e prestadores de serviço, anotá-las em meio físico exposto, mantê-las em arquivos sem criptografia ou permitir que sejam memorizadas em navegadores de equipamentos compartilhados. Quando houver necessidade de guarda de credenciais institucionais, esta será feita exclusivamente em cofre de senhas (gerenciador de credenciais) homologado, com acesso restrito e auditável, na forma prevista na seção "Recuperação de Desastres".

As contas com privilégios administrativos são nominais e de uso restrito às atividades que exijam tal nível de acesso, vedado o seu emprego em atividades rotineiras. Contas genéricas ou compartilhadas somente serão admitidas mediante justificativa técnica aprovada pelo CSI/RPP, com indicação de responsável e registro no inventário de ativos, e serão objeto de verificação na revisão semestral de permissões.

Em caso de esquecimento de senha, bloqueio ou qualquer outro problema de acesso, o colaborador deverá solicitar a redefinição à Gerência de Cadastro e Sistemas de Informação, que confirmará a identidade do solicitante antes de atender ao pedido, sendo vedado o atendimento de solicitações recebidas por meios não oficiais ou sem identificação segura. A senha redefinida terá caráter provisório e deverá ser alterada no primeiro acesso, e a solicitação e o atendimento serão registrados para fins de auditoria.

RIOPRETOPREV – Regime Próprio de Previdência Social do Município de São José do Rio Preto
Rua General Glicério, 3553 – Centro - CEP 15015-400 - São José do Rio Preto - SP Telefones (17) 3222 7445
E-mail: contato@riopretoprev.sp.gov.br - www.riopretoprev.sp.gov.br

Equipamentos

O colaborador é totalmente responsável por cada equipamento que usa, devendo zelar pelo seu estado de conservação, com especial atenção aos gabinetes de computadores.

Há uma relação de todos os equipamentos de informática vinculados a cada usuário, de acordo com o número do patrimônio. Qualquer troca de equipamento deve ser comunicada à administração para atualização desta lista.

Caso haja qualquer problema com algum dos equipamentos, este deve ser comunicado à Gerência de Cadastro e Sistemas de Informação para que a manutenção seja providenciada.

Excepcionalmente, havendo necessidade técnica de armazenamento temporário de informações no disco local do equipamento alocado ao usuário, este deve fazê-lo na área protegida do seu perfil, preferencialmente no diretório "Documentos", pois isso evita que outros usuários do mesmo equipamento tenham acesso a tais dados, providenciando, tão logo seja possível, a transferência do arquivo para um dos repositórios institucionais, vedada a guarda exclusiva em disco local.

Para uso de equipamentos compartilhados, como projetor e notebook, o motivo deve ser apresentado à Gerência de Cadastro e Sistemas de Informação, que providenciará os aparelhos, caso disponíveis para o evento requerido.

Durante o horário de uso, o responsável pela retirada responderá pelos equipamentos em sua posse.

Comportamento esperado (boas práticas)

Espera-se dos usuários da RIOPRETOPREV comportamento compatível com a PSI apresentada. Desta forma, são dadas a seguir algumas atitudes que devem ser observadas no dia a dia:

- Retirada dos papéis da impressora: toda vez que alguém enviar um documento para impressão, ele deve ser retirado imediatamente após ser impresso, de forma a evitar que fique exposto a terceiros;
- Descarte de papéis: caso algum papel com informação relevante e/ou confidencial necessite ser descartado, ele deve ser triturado na máquina específica para tal finalidade. Documentos confidenciais ou com dados pessoais de segurados não devem ser utilizados como papel de rascunho, devendo haver o descarte apropriado;
- Bloqueio da estação de trabalho: ao ausentar-se da frente de sua estação de trabalho sem bloquear a tela do computador, o usuário está aceitando o risco de um terceiro utilizar sua máquina sem autorização. Assim, o bloqueio deve ser feito após qualquer saída de frente da estação de trabalho. A proteção de tela também deve ser configurada para que o micro seja bloqueado após determinado período de inatividade;

- Conversas em áreas abertas: tal como não se deve divulgar informações da autarquia via internet, sem prévia autorização, também deve-se ter o cuidado de não divulgar, mesmo que de maneira não intencional, informações restritas. Desta forma, conversas sobre assuntos do trabalho (especialmente aquelas sensíveis e/ou que envolvam informações pessoais) devem ser evitadas em ambientes que possuam pessoas externas ou que possam comprometer a segurança das informações trocadas;
- Retirada de documentos da sede: não se deve retirar documentos da sede da RIOPRETOPREV, pois uma vez fora do prédio não é possível garantir seu correto tratamento. Caso haja a necessidade de locomoção dos documentos para reuniões externas ou viagens, a gerência responsável pela respectiva guarda deve ser informada.

RIOPRETOPREV – Regime Próprio de Previdência Social do Município de São José do Rio Preto
Rua General Glicério, 3553 – Centro - CEP 15015-400 - São José do Rio Preto - SP Telefones (17) 3222 7445
E-mail: contato@riopretoprev.sp.gov.br - www.riopretoprev.sp.gov.br

Gestão da Segurança da Informação

Em complemento à atuação colegiada da Comissão de Segurança da Informação (CSI/RPP), a RIOPRETOPREV mantém, no âmbito do ente federativo ou da própria Autarquia, servidor ou área responsável pela Gestão da Segurança da Informação, ao qual incumbe:

- prover todas as informações de Gestão de Segurança da Informação da unidade gestora do RPPS;
- prover ampla divulgação da Política e das Normas de Segurança da Informação a todos os servidores e prestadores de serviço;
- promover ações de conscientização sobre Segurança da Informação para servidores e prestadores de serviço;
- propor projetos e incentivos relacionados ao aperfeiçoamento da segurança da informação; e
- elaborar e manter a política de classificação da informação, com temporalidade para guarda, na forma da seção "Classificação da Informação" desta Política e da Tabela de Temporalidade e Destinação de Documentos aprovada pela Portaria nº 385/2020.

Dispositivos móveis

Considera-se dispositivo móvel qualquer aparelho ou mídia com característica de mobilidade, tais como notebook, smartphone, pendrive, CD e DVD.

Comumente, mídias como *pendrive* são usadas para transferir dados de um computador para outro. Apesar de ser recomendado usar o servidor de arquivos para tal finalidade, esta ação é permitida desde que todos os dados transferidos sejam apagados da mídia. Não havendo possibilidade de remoção (como em CD's e DVD's), a mídia usada deve ser descartada. O descarte deve ser feito através de sua destruição completa, seja por trituração ou manualmente.

A Empro disponibiliza rede Wi-Fi para acesso dos dispositivos, porém as regras estabelecidas para o uso da internet devem ser respeitadas, seja qual for o ponto de acesso, conforme o exposto na seção "Internet e VPN" deste documento.

Backup (cópia de segurança)

A RIOPRETOPREV adota estratégia de backup em múltiplas camadas para proteção dos seus ativos de informação, conforme detalhado no Manual do Procedimento de Contingência para Acesso às Cópias de Segurança dos Sistemas Informatizados e dos Bancos de Dados (versão 3.0, de agosto de 2026) e no Manual do Procedimento de Auditoria de Acesso e Rotinas de Recuperação de Desastres (versão 2.0, de agosto de 2026), este último acompanhado do Checklist de Teste de Restauração de Dados e da tabela de metas de RTO e RPO por sistema.

Backup dos Sistemas Críticos: As cópias de segurança dos sistemas críticos (Sistema de Gestão Previdenciária, Processo Digital, Atendimento e outros) são realizadas pelos fornecedores contratados, conforme cláusulas contratuais específicas que devem obrigatoriamente prever:

- Frequência de backup (no mínimo diário);
- Tipo de backup (completo, incremental ou diferencial);
- Local de armazenamento (offsite ou nuvem, com redundância geográfica);
- Metas de RTO (Tempo Objetivo de Recuperação) e RPO (Ponto Objetivo de Recuperação), conforme tabela aprovada pelo CSI/RPP.

Testes de Restauração: Os backups deverão ser testados com a seguinte periodicidade:

- Semestralmente: restauração de arquivos específicos (granular);
- Anualmente: simulação completa de recuperação de desastres (Full Disaster Recovery), com preenchimento do Checklist de Teste de Restauração e emissão de Relatório de Conformidade.

RIOPRETOPREV – Regime Próprio de Previdência Social do Município de São José do Rio Preto
Rua General Glicério, 3553 – Centro - CEP 15015-400 - São José do Rio Preto - SP Telefones (17) 3222 7445
E-mail: contato@riopretoprev.sp.gov.br - www.riopretoprev.sp.gov.br

Os testes serão executados em ambiente de homologação isolado da produção, sob supervisão do CSI/RPP, conforme procedimentos manualizados.

Backup de Estações de Trabalho: Os colaboradores devem armazenar seus arquivos de trabalho nos repositórios institucionais previstos na seção "Servidor de arquivos", preferencialmente no ambiente em nuvem do Microsoft 365 (OneDrive/SharePoint), que possui backup automático com redundância, ou no servidor de arquivos de rede provido pela Empro. É vedado o armazenamento exclusivo de arquivos institucionais no disco local da estação de trabalho. Arquivos de e-mail (Outlook) são armazenados em nuvem pelo Microsoft 365, dispensando backup local pelo usuário.

Não é permitido realizar backup de dados institucionais em equipamentos ou mídias pessoais.

Auditoria de Acesso

A auditoria de acesso é componente essencial da gestão da segurança da informação, assegurando que sistemas e dados estejam protegidos contra acessos não autorizados, observado o disposto no Manual do Procedimento de Controle de Acesso Lógico aos Sistemas e Bancos de Dados (versão 3.0, de agosto de 2026), que mapeia e manualiza todo o ciclo de vida da credencial, da solicitação e verificação de atribuições à concessão, à alteração por movimentação, à revogação por desligamento e à revisão semestral de permissões e contas órfãs, e no Manual do Procedimento de Auditoria de Acesso e Rotinas de Recuperação de Desastres (versão 2.0, de agosto de 2026), que disciplina o ciclo semestral de auditoria e a emissão do Relatório de Auditoria de Acessos. O CSI/RPP, em articulação com a Gerência de Cadastro e Sistemas de Informação e com as empresas fornecedoras dos sistemas, adota os seguintes procedimentos:

a) Definição de Políticas de Acesso

São estabelecidas políticas formais de acesso, definindo quem pode acessar quais dados e sistemas, com base nas atribuições de cada usuário e observados os princípios do menor privilégio e da segregação de funções.

b) Revisão Regular de Permissões

As permissões de acesso são revisadas periodicamente, no mínimo semestralmente, assegurando-se que as credenciais estejam alinhadas às responsabilidades atuais do usuário e que os acessos de servidores desligados ou remanejados sejam revogados tempestivamente, evitando o acúmulo indevido de privilégios.

a. **Revogação Imediata de Acesso**

Independentemente da revisão periódica de que trata a alínea anterior, os acessos lógicos e físicos serão revogados de imediato, na data em que o evento produzir efeitos ou, quando a ciência for posterior, no primeiro dia útil seguinte, nas seguintes hipóteses:

- Exoneração, demissão, aposentadoria, falecimento, término de estágio ou qualquer outra forma de desligamento do servidor ou colaborador;
- Encerramento, rescisão ou suspensão de contrato de prestação de serviços, bem como substituição de preposto, empregado ou técnico da contratada que detenha credenciais de acesso;
- Remanejamento, cessão, mudança de lotação ou alteração de função, hipótese em que a revogação alcança exclusivamente os acessos incompatíveis com as novas atribuições;
- Afastamento ou licença de duração superior a 30 (trinta) dias, caso em que os acessos serão suspensos e restabelecidos por ocasião do retorno;
- Determinação do CSI/RPP em razão de incidente de segurança, de suspeita de comprometimento ou de uso indevido de credenciais.

A área de gestão de pessoas, quanto aos servidores e estagiários, e o gestor do contrato, quanto aos prestadores de serviço, comunicarão o evento à Gerência de Cadastro e Sistemas de Informação e ao CSI/RPP, preferencialmente com antecedência e, no mínimo, na data em que ele produzir efeitos. A comunicação e a confirmação da execução serão registradas no sistema de processo digital e constituem evidência do procedimento para fins de auditoria.

A revogação abrange todos os meios de acesso vinculados ao usuário, notadamente a conta de rede e o diretório corporativo; os serviços do Microsoft 365, incluindo correio eletrônico, OneDrive, SharePoint e

RIOPRETOPREV – Regime Próprio de Previdência Social do Município de São José do Rio Preto
Rua General Glicério, 3553 – Centro - CEP 15015-400 - São José do Rio Preto - SP Telefones (17) 3222 7445
E-mail: contato@riopretoprev.sp.gov.br - www.riopretoprev.sp.gov.br

Teams; a VPN e demais formas de acesso remoto; o sistema de gestão previdenciária e os bancos de dados; o sistema de processo digital; a plataforma do canal corporativo de atendimento por WhatsApp; os demais sistemas corporativos e serviços providos por terceiros; os certificados e tokens de assinatura vinculados à função; e o crachá e as credenciais de acesso físico, com a devolução dos equipamentos e dispositivos sob responsabilidade do usuário.

As contas serão bloqueadas, e não excluídas de imediato, preservando-se o conteúdo institucional, as caixas postais e os registros de acesso pelos prazos de guarda aplicáveis. Os arquivos e as mensagens de interesse da Autarquia serão transferidos ao gestor imediato ou ao substituto designado, mediante registro, e o correio eletrônico poderá ser redirecionado pelo período necessário à continuidade do serviço. A exclusão definitiva da conta depende de autorização do CSI/RPP, observados os prazos de guarda e a inexistência de apuração em curso.

Quando a revogação depender de fornecedor externo ou de prestador de serviços de tecnologia, a solicitação formal será encaminhada no mesmo dia, cabendo à Gerência de Cadastro e Sistemas de Informação acompanhar o cumprimento e registrar a data de execução. Enquanto não confirmada a revogação, o acesso permanecerá suspenso por bloqueio da credencial ou por outra medida de contenção disponível.

c) **Monitoramento em Tempo Real**

São utilizadas ferramentas de monitoramento para identificar atividades suspeitas, tais como tentativas de acesso não autorizado, alterações indevidas de permissões e padrões de comportamento anômalos.

d) **Registro de Auditoria**

São mantidos registros (logs) detalhados das atividades de acesso, contendo, no mínimo, a identificação do usuário ou do serviço, a data e a hora do evento, o endereço de origem, o sistema ou recurso acessado, a operação realizada e o resultado da tentativa. Os relógios dos sistemas e servidores devem ser sincronizados a partir de fonte de tempo confiável, de modo a assegurar a correlação dos eventos.

Os registros são armazenados de forma íntegra e protegida contra adulteração e observam os seguintes prazos mínimos de retenção:

Categoria de registro	Prazo mínimo de retenção
Registros de acesso e de operações nos sistemas críticos, assim considerados o sistema de gestão previdenciária, o processo digital, o sistema de atendimento e os respectivos bancos de dados	5 (cinco) anos
Registros de uso de contas com privilégios administrativos e de alterações de permissões, de perfis e de parametrizações	5 (cinco) anos
Registros de concessão, alteração e revogação de acessos e Relatórios de Auditoria de Acessos	5 (cinco) anos
Registros de ingresso de não servidores em áreas sensíveis	5 (cinco) anos
Registros de autenticação, incluindo tentativas malsucedidas, bloqueios de conta e redefinições de senha	12 (doze) meses
Registros de acesso remoto por VPN e demais tecnologias de acesso à distância	12 (doze) meses
Registros de infraestrutura, de rede, de correio eletrônico e de estações de trabalho	12 (doze) meses

RIOPRETOPREV – Regime Próprio de Previdência Social do Município de São José do Rio Preto
Rua General Glicério, 3553 – Centro - CEP 15015-400 - São José do Rio Preto - SP Telefones (17) 3222 7445
E-mail: contato@riopretoprev.sp.gov.br - www.riopretoprev.sp.gov.br

Registros relacionados a incidente de segurança da informação, contados do encerramento do incidente	5 (cinco) anos

Os prazos previstos nesta seção são mínimos e não afastam prazos superiores fixados no Código de Classificação e na Tabela de Temporalidade e Destinação de Documentos da RIOPRETOPREV, aprovados pela Portaria nº 385/2020, em especial na classe 068 – Segurança da Informação, nem prazos determinados por legislação específica, por órgão de controle ou por decisão judicial, hipóteses em que prevalece o prazo mais longo.

É vedada a alteração, a exclusão ou a sobreposição de registros antes do decurso do prazo aplicável. Havendo apuração de incidente, procedimento disciplinar, auditoria, fiscalização ou litígio em curso, os registros pertinentes serão preservados até o encerramento definitivo, ainda que ultrapassado o prazo de retenção. O acesso aos registros é restrito aos servidores autorizados e às atividades de auditoria, é ele próprio registrado e observa a classificação da informação e a proteção dos dados pessoais neles contidos.

Os registros são revisados periodicamente, no mínimo por ocasião do ciclo semestral de auditoria de acessos, para a detecção de eventuais violações de segurança. Quando os registros forem mantidos por fornecedores de sistemas ou de infraestrutura, os prazos e as condições de guarda, de integridade e de disponibilização à Autarquia constarão de cláusula contratual, na forma da seção "Gestão de Fornecedores e Terceiros", cabendo à Gerência de Cadastro e Sistemas de Informação verificar o seu cumprimento.

e) **Testes de Penetração**

São realizados testes de vulnerabilidade e, quando aplicável, testes de intrusão, com periodicidade mínima anual ou sempre que houver mudança relevante nos sistemas, a fim de identificar fragilidades nos controles de acesso frente a ameaças externas e internas.

f) **Treinamento de Usuários**

São promovidas ações periódicas de capacitação e conscientização dos usuários sobre práticas seguras de acesso, incluindo o uso de senhas robustas, a autenticação multifator (MFA) e a identificação de tentativas de phishing e de engenharia social.

Recuperação de Desastres

A recuperação de desastres é parte crítica do plano de continuidade dos serviços, visando minimizar o impacto de eventos adversos. São implementadas, com o apoio da empresa Empro Tecnologia e Informação (Empro), as rotinas a seguir, detalhadas no Manual do Procedimento de Auditoria de Acesso e Rotinas de Recuperação de Desastres (versão 2.0, de agosto de 2026):

a) Análise de Riscos

É realizada análise abrangente de riscos para identificar potenciais ameaças que possam afetar os sistemas e as operações, incluindo desastres naturais, falhas de hardware, ataques cibernéticos e outros eventos imprevistos.

b) Backup Regular

É implementado plano de backup regular e automatizado para todos os dados críticos. Essas cópias de segurança são armazenadas de forma segura em locais geograficamente distintos, para garantir a disponibilidade dos dados em caso de perda.

c) Procedimentos de Recuperação

São desenvolvidos procedimentos detalhados de recuperação para cada sistema e conjunto de dados, incluindo a sequência de passos para restaurar sistemas, aplicativos e dados essenciais a partir das cópias de segurança.

d) Testes Periódicos

RIOPRETOPREV – Regime Próprio de Previdência Social do Município de São José do Rio Preto
Rua General Glicério, 3553 – Centro - CEP 15015-400 - São José do Rio Preto - SP Telefones (17) 3222 7445
E-mail: contato@riopretoprev.sp.gov.br - www.riopretoprev.sp.gov.br

São realizados testes dos procedimentos de recuperação de desastres, no mínimo anualmente, em consonância com a simulação completa (Full Disaster Recovery) prevista na seção de Backup, para assegurar sua execução efetiva quando necessário e avaliar a eficácia do plano.

e) Identificação de Pessoal-Chave

É mantida lista atualizada do pessoal-chave responsável pela execução do plano de recuperação, assegurando-se que cada integrante conheça suas responsabilidades em situação de desastre.

f) Comunicação de Emergência

São estabelecidos protocolos de comunicação de emergência para garantir comunicação rápida e eficaz entre os envolvidos durante um evento de recuperação de desastres.

g) Armazenamento de Documentação

São documentadas todas as informações relevantes, incluindo configurações de sistemas, procedimentos de recuperação e contatos de fornecedores. Eventuais credenciais de recuperação são guardadas exclusivamente em cofre de senhas (gerenciador de credenciais), com acesso restrito e auditável, vedado o armazenamento de senhas em texto claro. A documentação é mantida de forma segura e acessível ao pessoal autorizado.

h) Atualização Contínua

O plano de recuperação de desastres é revisado e atualizado regularmente, de modo a refletir mudanças na infraestrutura de TI, na equipe e no cenário de ameaças.

Assinatura e processo digital

Todos os servidores da RIOPRETOPREV possuem *token* de identificação pessoal certificado, usado para assinaturas digitais de documentos em geral, podendo incluir e-mails.

Tal como já apontado na seção "Identificação pessoal", seu uso é pessoal e intransferível, sendo vedado qualquer tipo de cessão a outras pessoas.

A assinatura realizada com o dispositivo tem validade legal e, portanto, sua utilização deve se dar da mesma forma que o uso da assinatura em papel, devendo-se avaliar bem o documento sendo assinado.

Para assinatura digital, deve-se introduzir o *token* na estação de trabalho e, através do software que manipula o documento alvo, realizar os comandos para assinatura, introduzindo, quando solicitado, o valor de PIN (senha) do referido *token*. Recomenda-se que o valor do PIN seja alterado para que fique diferente da senha padrão fornecida inicialmente. Havendo dúvidas de como proceder nesta operação, a Gerência de Cadastro e Sistemas de Informação deve ser consultada.

A principal utilidade do referido dispositivo é a validação dos documentos e despachos do processo digital implantado na autarquia. Para uso desta funcionalidade, os colaboradores devem realizar seu acesso ao site 'riopretoprev.1doc.com.br', mantendo suas informações pessoais atualizadas e tramitando os processos de acordo com os respectivos mapeamentos.

Da mesma forma, as credenciais de acesso ao site são pessoais e intransferíveis, devendo o usuário zelar pela sua confidencialidade, bem como pela integridade de todas as informações ali contidas, sejam de processos de próprio interesse ou de processos de terceiros de que venha a ter conhecimento.

Além da assinatura por token físico (certificado ICP-Brasil), a RIOPRETOPREV reconhece como válidas as assinaturas eletrônicas realizadas por meio da plataforma de processo digital (1Doc), desde que o signatário esteja devidamente autenticado com suas credenciais pessoais e, quando disponível, com autenticação multifator (MFA). As credenciais de acesso à plataforma 1Doc são pessoais e intransferíveis, devendo o usuário zelar pela sua confidencialidade e comunicar imediatamente ao CSI/RPP qualquer suspeita de uso indevido.

RIOPRETOPREV – Regime Próprio de Previdência Social do Município de São José do Rio Preto
Rua General Glicério, 3553 – Centro - CEP 15015-400 - São José do Rio Preto - SP Telefones (17) 3222 7445
E-mail: contato@riopretoprev.sp.gov.br - www.riopretoprev.sp.gov.br

Classificação da Informação

A informação custodiada pela RIOPRETOPREV deve ser classificada quanto ao grau de sigilo, de modo a orientar os controles de proteção, as regras de compartilhamento e o tempo de guarda, em observância à Lei nº 12.527/2011 (Lei de Acesso à Informação), à Lei nº 13.709/2018 (LGPD) e ao item 3.1.5 do Manual do Pró-Gestão RPPS.

Para os fins desta Política, as informações são classificadas nos seguintes níveis:

Pública: informações que podem ser livremente divulgadas, sem prejuízo à Autarquia ou a terceiros.

Interna: informações de uso interno cuja divulgação não autorizada não causa dano relevante, mas que não se destinam ao público externo.

Restrita: informações cujo acesso é limitado a grupos específicos de servidores, em razão da função, e cuja divulgação indevida pode causar dano à Autarquia ou a terceiros.

Sigilosa/Confidencial: informações pessoais e sensíveis de segurados e beneficiários, dados protegidos por sigilo legal e informações estratégicas, cuja divulgação não autorizada pode causar dano significativo ou violar direitos dos titulares.

A responsabilidade pela classificação é do servidor que produz ou recebe a informação, sob orientação do gestor da respectiva área e do CSI/RPP. Os controles de acesso, transmissão, armazenamento e descarte devem ser proporcionais ao nível de classificação, observando-se, para as informações restritas e sigilosas, o princípio do menor privilégio, a criptografia quando aplicável e o registro de acesso.

A definição dos prazos de guarda e da destinação final dos documentos observa o Código de Classificação e a Tabela de Temporalidade e Destinação de Documentos da RIOPRETOPREV (versão 1.0, de setembro de 2020), aprovados pela Portaria nº 385/2020, que contempla, entre outras, a classe 068 – Segurança da Informação (incluído o subgrupo 068.1 – Incidente de Segurança da Informação). A classificação quanto ao sigilo prevista nesta seção é complementar àquele instrumento e à seção "Arquivos digitalizados", cabendo à Gerência de Cadastro e Sistemas de Informação, em apoio ao CSI/RPP, orientar a aplicação conjunta.

Arquivos digitalizados

A digitalização de documentos para a RIOPRETOPREV deve seguir o disposto no Decreto Federal nº 10.278, de 18 de março de 2020, observados o Código de Classificação e a Tabela de Temporalidade e Destinação de Documentos da RIOPRETOPREV, aprovados pela Portaria nº 385/2020.

O colaborador que for designado para a operação de digitalização dos documentos deve ter conhecimento da sua confidencialidade, zelando para que ninguém mais tenha acesso ao documento, se não for pessoa de interesse.

A digitalização deve ser realizada mediante o software proprietário provindo da mesma fabricante da máquina digitalizadora. Quando isto não for aplicável, a Gerência de Cadastro e Sistemas de Informação é a responsável por indicar e instalar eventual software substituto. Os parâmetros utilizados para tal devem ser configurados pela referida Gerência no computador do usuário.

Os dados e metadados do arquivo gerado são de responsabilidade do digitalizador e do detentor do documento. Tais informações devem ser cadastradas por meio de software próprio para edição de metadados, a ser indicado pela Gerência de Cadastro e Sistemas de Informação. A transferência do arquivo gerado com os metadados do local de digitalização para o local de armazenamento deve ser realizada dentro da rede protegida, utilizando os repositórios institucionais, visto que tanto o arquivo quanto seus metadados podem possuir informações sigilosas ou confidenciais.

Todo documento físico que for movido de lugar para a digitalização deve ser retornado à sua origem, quando o procedimento for concluído, para sua devida destinação.

Da Política de Privacidade de Dados Pessoais

RIOPRETOPREV – Regime Próprio de Previdência Social do Município de São José do Rio Preto
Rua General Glicério, 3553 – Centro - CEP 15015-400 - São José do Rio Preto - SP Telefones (17) 3222 7445
E-mail: contato@riopretoprev.sp.gov.br - www.riopretoprev.sp.gov.br

A RIOPRETOPREV edita e mantém Política de Privacidade de Dados Pessoais específica, na qual detalha a coleta, o uso, a proteção dos dados pessoais e os direitos dos titulares, devendo tal política permanecer disponível para consulta no sítio eletrônico da Autarquia.

a) Quais os tipos de informações pessoais são coletados.
b) Como essas informações são usadas e processadas.
c) Quais medidas são tomadas para proteger essas informações.
d) Os direitos e opções dos indivíduos em relação a suas informações pessoais.
e) Procedimentos para solicitações de acesso, correção e exclusão de informações pessoais.
f) Responsabilidades da RIOPRETOPREV em relação à política.

A RIOPRETOPREV designa formalmente, por ato próprio, o Encarregado pelo Tratamento de Dados Pessoais (DPO), nos termos do art. 41 da Lei nº 13.709/2018, cuja identidade e canal de contato são divulgados na Política de Privacidade e no sítio eletrônico da Autarquia. Ao Encarregado compete atuar como canal de comunicação entre a Autarquia, os titulares e a Autoridade Nacional de Proteção de Dados (ANPD), articulando-se com o CSI/RPP no tratamento de incidentes que envolvam dados pessoais.

A RIOPRETOPREV mantém e conserva atualizado o Registro das Operações de Tratamento de Dados Pessoais (ROPA), nos termos do art. 37 da Lei nº 13.709/2018, contemplando as finalidades, as bases legais, as categorias de dados e de titulares, os compartilhamentos e os prazos de guarda, sob a coordenação do Encarregado (DPO) e em articulação com o CSI/RPP, sendo revisado sempre que houver alteração relevante nas operações de tratamento.

Uso de Inteligência Artificial

A RIOPRETOPREV autoriza e incentiva o uso de ferramentas de Inteligência Artificial (IA) institucionais, como o Microsoft Copilot, para aumento da produtividade e qualidade dos serviços prestados.

O uso de Inteligência Artificial na RIOPRETOPREV observa os princípios da supervisão humana significativa, da responsabilização, da transparência, da não discriminação, da explicabilidade e da proteção de dados pessoais, em consonância com a Lei nº 13.709/2018 (LGPD), com as orientações da Autoridade Nacional de Proteção de Dados (ANPD) sobre tratamento automatizado de dados e com as diretrizes de uso responsável de IA no setor público, notadamente o Guia de Uso de Inteligência Artificial Generativa do Tribunal de Contas da União (TCU). A IA constitui ferramenta de apoio à atividade do servidor, não substituindo o seu juízo funcional; o servidor permanece integralmente responsável pelo conteúdo que produz com auxílio de IA e por sua conformidade jurídica e técnica.

Ao utilizar ferramentas de IA, o colaborador deverá observar as seguintes regras:

- Utilizar preferencialmente as ferramentas de IA autorizadas pela Autarquia e disponibilizadas no ambiente corporativo, priorizando soluções institucionais ou homologadas pela Gerência de Cadastro e Sistemas de Informação e pelo CSI/RPP;
- Formular solicitações de forma objetiva, clara e limitada à finalidade de trabalho, evitando incluir dados pessoais, dados sensíveis, informações identificáveis, estratégicas, sigilosas, protegidas por lei ou internas que não sejam estritamente necessárias;
- Utilizar, sempre que possível, exemplos fictícios, informações públicas ou dados anonimizados, especialmente em testes, minutas, simulações, treinamentos ou estudos preliminares;
- Não inserir em ferramentas de IA externas ou não autorizadas dados pessoais de segurados, beneficiários, servidores ou terceiros, informações financeiras, senhas, dados de processos administrativos, documentos internos ou qualquer informação classificada como restrita, sigilosa ou confidencial;
- Não utilizar o e-mail institucional, telefone corporativo ou outras credenciais da Autarquia para cadastro em ferramentas de IA externas não homologadas;

RIOPRETOPREV – Regime Próprio de Previdência Social do Município de São José do Rio Preto
Rua General Glicério, 3553 – Centro - CEP 15015-400 - São José do Rio Preto - SP Telefones (17) 3222 7445
E-mail: contato@riopretoprev.sp.gov.br - www.riopretoprev.sp.gov.br

- Utilizar a resposta gerada pela IA apenas como apoio, nunca como produto automático, devendo o servidor revisar criticamente o conteúdo, verificar fatos, conferir fundamentos legais, atualizar referências e adequar a redação ao contexto institucional da RIOPRETOPREV;
- Considerar que ferramentas de IA podem produzir informações incorretas, desatualizadas, inventadas ou enviesadas, inclusive referências normativas inexistentes, interpretações jurídicas inadequadas e conclusões aparentemente neutras, mas incompatíveis com o caso concreto;
- Não utilizar ferramentas de IA para substituir análise técnica, jurídica, administrativa ou previdenciária, nem para tomada de decisões estratégicas, atos administrativos, julgamentos individualizados ou decisões automatizadas que afetem direitos de segurados e beneficiários sem supervisão humana significativa;
- Assegurar, quando aplicável, o direito à revisão humana de decisões baseadas em tratamento automatizado de dados pessoais, nos termos do art. 20 da Lei nº 13.709/2018;
- Manter, sempre que possível, registro do uso institucional de IA, indicando finalidade, ferramenta utilizada, versão ou ambiente, principais comandos empregados, responsável pela revisão humana e eventuais ajustes realizados antes da utilização oficial;
- Não implementar códigos, rotinas, fórmulas, macros, integrações, automações ou divulgar links sugeridos por IA sem revisão técnica especializada e validação pela área competente;
- Não utilizar diretamente conteúdo gerado por IA em comunicações oficiais, publicações externas, respostas a órgãos de controle, atos administrativos ou documentos destinados ao público externo sem revisão, validação institucional e assunção expressa de responsabilidade pelo servidor competente;
- Observar transparência proporcional ao risco e à finalidade, informando, sempre que pertinente, que determinado conteúdo foi elaborado com apoio de IA, sem prejuízo da responsabilidade integral do servidor pela versão final;
- Não inserir em ferramentas de IA conteúdos protegidos por direitos autorais ou por sigilo sem autorização, nem apresentar como produto institucional, sem revisão e validação, conteúdo integralmente gerado por IA;
- Comunicar imediatamente ao CSI/RPP e ao Encarregado de Dados qualquer comportamento anômalo, suspeita de vazamento, exposição indevida de dados, resposta potencialmente discriminatória, uso malicioso, tentativa de engenharia social ou incidente relacionado ao uso de IA.

A utilização de IA deve ser precedida de avaliação mínima de adequação da ferramenta à tarefa. Atividades de apoio, como organização de ideias, revisão linguística, elaboração de minutas preliminares, consolidação de informações públicas e estruturação de documentos, podem ser compatíveis com o uso de IA, desde que preservada a revisão humana. Por outro lado, tarefas que envolvam decisões estratégicas, atos administrativos finais, avaliação individual de direitos, tratamento de informações sigilosas, definição de entendimentos jurídicos ou previdenciários e comunicação institucional sensível exigem cautela reforçada e validação pela autoridade competente.

O uso inadequado de IA pode gerar riscos institucionais relevantes, incluindo vazamento de dados, incidentes de segurança, reprodução de vieses, desinformação, decisões baseadas em conteúdo incorreto ou desatualizado, violação da LGPD, de direitos autorais ou de normas administrativas, além de perda de confiança pública e questionamentos por órgãos de controle. A aparência de neutralidade ou precisão do conteúdo gerado não dispensa verificação técnica, jurídica e contextual.

A adoção de novas ferramentas de IA, internas ou externas, depende de prévia homologação pela Gerência de Cadastro e Sistemas de Informação e pelo CSI/RPP, que manterá relação atualizada das soluções autorizadas e reavaliará periodicamente os riscos associados ao seu uso, inclusive quanto à proteção de dados pessoais, segurança da informação, rastreabilidade, transparência, vieses, imprecisões, alucinações, obsolescência das respostas, possibilidade de uso malicioso e aderência ao contexto brasileiro e institucional da RIOPRETOPREV.

RIOPRETOPREV – Regime Próprio de Previdência Social do Município de São José do Rio Preto
Rua General Glicério, 3553 – Centro - CEP 15015-400 - São José do Rio Preto - SP Telefones (17) 3222 7445
E-mail: contato@riopretoprev.sp.gov.br - www.riopretoprev.sp.gov.br

Resposta a Incidentes de Segurança da Informação

A RIOPRETOPREV adota procedimento estruturado para tratamento de incidentes de segurança da informação, conduzido pelo CSI/RPP em articulação com o Encarregado de Dados (DPO).

Definição: Considera-se incidente de segurança da informação qualquer evento adverso, confirmado ou sob suspeita, que comprometa a confidencialidade, integridade ou disponibilidade de dados ou sistemas da Autarquia, incluindo, mas não se limitando a: acessos não autorizados, vazamento de dados pessoais, infecção por malware, perda ou furto de equipamentos, indisponibilidade prolongada de sistemas e envio indevido de informações.

Comunicação: Todo colaborador que identificar ou suspeitar de um incidente deverá comunicá-lo imediatamente ao CSI/RPP e ao Encarregado de Dados, por meio dos canais oficiais, fornecendo o máximo de detalhes disponíveis (data/hora, sistemas afetados, tipo de incidente, dados potencialmente expostos).

Tratamento: O CSI/RPP, ao receber a comunicação, deverá:

- Classificar o incidente quanto à gravidade (baixo, médio, alto, crítico);
- Adotar medidas imediatas de contenção;
- Investigar a causa raiz;
- Registrar o incidente no sistema de processo digital;
- Comunicar à Diretoria e, quando envolver dados pessoais com risco relevante aos titulares, à ANPD e aos titulares afetados, nos termos da LGPD;
- Propor medidas corretivas e preventivas para evitar recorrência.

Registro e Aprendizado: Todos os incidentes, independentemente da gravidade, deverão ser registrados em relatório específico para fins de auditoria, aprendizado organizacional e melhoria contínua dos controles de segurança.

Tratando-se de incidente de segurança que envolva dados pessoais e possa acarretar risco ou dano relevante aos titulares, a comunicação à Autoridade Nacional de Proteção de Dados (ANPD) e aos titulares afetados será realizada, por meio do Encarregado (DPO), no prazo de 3 (três) dias úteis contados do conhecimento de que o incidente afetou dados pessoais, nos termos da Resolução CD/ANPD nº 15/2024, ressalvada a existência de prazo diverso em legislação específica.

O registro do incidente, inclusive daquele não comunicado à ANPD e aos titulares, será mantido pelo prazo mínimo de 5 (cinco) anos, em consonância com a Resolução CD/ANPD nº 15/2024 e com a classe 068.1 (Incidente de Segurança da Informação) da Tabela de Temporalidade da RIOPRETOPREV.

Proteção de Endpoint e Antivírus

Todas as estações de trabalho e servidores da RIOPRETOPREV devem possuir solução de antivírus/antimalware ativa e atualizada, conforme especificações definidas pela Gerência de Cadastro e Sistemas de Informação.

É vedado ao colaborador:

- Desabilitar, desinstalar ou alterar as configurações do software de proteção;
- Ignorar alertas de segurança emitidos pelo software;
- Conectar dispositivos removíveis (pendrives, HDs externos) sem prévia verificação pelo antivírus.

As atualizações de segurança do sistema operacional e dos softwares instalados deverão ser aplicadas de forma automática ou, quando isso não for possível, no prazo máximo de 72 horas após a disponibilização pelo fabricante.

Controle de Acesso Físico

O controle de acesso físico complementa o controle de acesso lógico e tem por objetivo proteger as dependências, os equipamentos e os ativos de informação da RIOPRETOPREV contra acessos não

RIOPRETOPREV – Regime Próprio de Previdência Social do Município de São José do Rio Preto
Rua General Glicério, 3553 – Centro - CEP 15015-400 - São José do Rio Preto - SP Telefones (17) 3222 7445
E-mail: contato@riopretoprev.sp.gov.br - www.riopretoprev.sp.gov.br

autorizados, danos e interferências, na forma mapeada e manualizada no Manual do Procedimento de Controle de Acesso Físico às Dependências, Áreas Sensíveis e Ativos de Informação (versão 3.0, de agosto de 2026), que disciplina, inclusive, o registro obrigatório de ingresso de não servidores em áreas sensíveis, com indicação da área acessada, do motivo, do responsável pela autorização, do acompanhante e dos horários de entrada e de saída.

O ingresso e a permanência nas dependências da RIOPRETOPREV e em todas as suas áreas internas são permitidos exclusivamente a servidores e colaboradores devidamente identificados por crachá ou credencial funcional, de uso pessoal e intransferível, que deverá ser portado de forma visível durante toda a permanência nas instalações.

Os visitantes deverão ser previamente identificados e registrados, receber identificação temporária e permanecer acompanhados por servidor responsável, sendo-lhes vedado o acesso às áreas restritas.

Constituem áreas restritas, entre outras, a sala de servidores e de equipamentos de rede e os locais de guarda de documentos físicos com informações restritas ou sigilosas, cujo acesso é limitado aos servidores expressamente autorizados, com registro de entrada e saída. Quando a infraestrutura de servidores estiver hospedada em ambiente de terceiro (Empro), o controle de acesso físico observará as condições contratuais e os controles do prestador.

Inventário de Ativos de Informação

A RIOPRETOPREV mantém inventário atualizado de seus ativos de informação, compreendendo, entre outros, os sistemas e bases de dados, os documentos físicos e digitais, os equipamentos e a infraestrutura de rede, bem como os serviços de tratamento de dados prestados por terceiros.

Cada ativo possui um responsável (gestor do ativo) identificado, ao qual cabe zelar por sua proteção e por sua correta classificação, nos termos da seção “Classificação da Informação”.

O inventário registra, no mínimo, a identificação do ativo, seu responsável, sua classificação quanto ao sigilo e o respectivo custodiante, é revisado periodicamente e constitui insumo essencial para a gestão de riscos e para o controle de acesso.

Gestão de Riscos de Segurança da Informação

O CSI/RPP mantém processo contínuo de gestão de riscos de segurança da informação, com o objetivo de identificar, avaliar, tratar e monitorar os riscos a que estão sujeitos os ativos de informação da Autarquia.

A análise de riscos compreende a identificação dos ativos, das ameaças e das vulnerabilidades a eles associadas e a estimativa do risco a partir da combinação entre a probabilidade de ocorrência e o impacto potencial sobre a confidencialidade, a integridade e a disponibilidade da informação.

Os riscos são hierarquizados em uma matriz de probabilidade e impacto, classificados nos níveis **Baixo, Médio, Alto e Crítico**, e tratados conforme uma das seguintes estratégias: mitigar (implantar controles que reduzam o risco), transferir (compartilhar o risco, por exemplo, mediante contrato ou seguro), aceitar (assumir formalmente o risco residual, mediante justificativa registrada) ou evitar (eliminar a atividade que origina o risco). Os riscos classificados como Alto ou Crítico exigem plano de tratamento com responsável e prazo definidos.

A análise de riscos é registrada em matriz própria, revisada no mínimo anualmente e sempre que ocorrerem mudanças relevantes na infraestrutura, nos processos, nos fornecedores críticos ou no cenário de ameaças, e seus resultados são submetidos à apreciação do CSI/RPP.

Gestão de Fornecedores e Terceiros

Parte relevante dos serviços e do tratamento de dados pessoais da RIOPRETOPREV é executada por terceiros (operadores), tais como os responsáveis pelo sistema de gestão previdenciária, pelo processo digital e

RIOPRETOPREV – Regime Próprio de Previdência Social do Município de São José do Rio Preto
Rua General Glicério, 3553 – Centro - CEP 15015-400 - São José do Rio Preto - SP Telefones (17) 3222 7445
E-mail: contato@riopretoprev.sp.gov.br - www.riopretoprev.sp.gov.br

pelo armazenamento de dados. A Autarquia gerencia os riscos de segurança da informação ao longo dessa cadeia, na condição de controladora dos dados.

Os contratos e termos de adesão firmados com fornecedores que acessem, armazenem ou tratem informações da RIOPRETOPREV deverão conter cláusulas de segurança da informação e de proteção de dados, definindo, no mínimo: as responsabilidades das partes; o dever de confidencialidade; a obrigação de comunicar incidentes de segurança em prazo compatível com o desta Política e com a Resolução CD/ANPD nº 15/2024; e o direito de a Autarquia auditar o cumprimento dessas obrigações.

Previamente à contratação, deverá ser verificado o atendimento, pelo fornecedor, dos requisitos mínimos de segurança da informação compatíveis com a criticidade dos dados e serviços envolvidos.

O operador somente poderá tratar os dados conforme as instruções e as finalidades contratadas, sendo vedado o uso para finalidade diversa. Ao término do contrato, os dados deverão ser devolvidos à RIOPRETOPREV ou eliminados de forma segura, conforme orientação da Autarquia, nos termos dos arts. 15, 16 e 39 da Lei nº 13.709/2018. Os operadores em atividade são identificados na Política de Privacidade da RIOPRETOPREV.

Termo de Responsabilidade

Como condição para o acesso às informações e aos recursos tecnológicos da RIOPRETOPREV, os servidores, estagiários, prestadores de serviço e demais colaboradores deverão firmar Termo de Responsabilidade e Confidencialidade, por meio do qual declaram conhecer e se comprometem a observar esta Política de Segurança da Informação.

O Termo observa o modelo constante do Anexo I do Manual do Procedimento de Controle de Acesso Lógico aos Sistemas e Bancos de Dados (versão 3.0, de agosto de 2026) e será firmado no momento da admissão ou do início da prestação dos serviços e renovado sempre que houver alteração relevante nesta Política, ficando arquivado sob responsabilidade do CSI/RPP, em articulação com a área de gestão de pessoas e com os gestores dos contratos.

O descumprimento desta Política sujeita o infrator às sanções administrativas, disciplinares, contratuais e legais cabíveis, sem prejuízo das responsabilidades civis e penais e das penalidades previstas na Lei nº 13.709/2018, apuradas mediante o devido processo legal.

Referências Normativas

Esta Política observa, no que couber, as seguintes normas e referências:

- Constituição Federal de 1988 (art. 5º e art. 37) e Emenda Constitucional nº 103/2019.
- Lei nº 9.717/1998 — normas gerais de organização e funcionamento dos RPPS.
- Lei nº 12.527/2011 — Lei de Acesso à Informação (LAI).
- Lei nº 13.709/2018 — Lei Geral de Proteção de Dados Pessoais (LGPD).
- Resolução CD/ANPD nº 15/2024 — regulamenta a comunicação de incidente de segurança com dados pessoais à Autoridade Nacional de Proteção de Dados e aos titulares.
- Decreto Federal nº 10.278/2020 — técnica e requisitos para a digitalização de documentos públicos ou privados.
- Portaria nº 385/2020 — aprova o Código de Classificação e a Tabela de Temporalidade e Destinação de Documentos da RIOPRETOPREV.
- Portaria MTP nº 1.467/2022 — parâmetros e diretrizes gerais aplicáveis aos RPPS.
- Manual do Pró-Gestão RPPS, item 3.1.5 - Política de Segurança da Informação, versão aplicável ao ciclo de certificação.
- ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 — sistema de gestão e controles de segurança da informação.

RIOPRETOPREV – Regime Próprio de Previdência Social do Município de São José do Rio Preto
Rua General Glicério, 3553 – Centro - CEP 15015-400 - São José do Rio Preto - SP Telefones (17) 3222 7445
E-mail: contato@riopretoprev.sp.gov.br - www.riopretoprev.sp.gov.br

- Guia de Uso de Inteligência Artificial Generativa do Tribunal de Contas da União (TCU) — diretrizes de uso responsável de IA no setor público.
- Regimento Interno do CSI/RPP e Código de Ética da RIOPRETOPREV.
- Manuais internos de procedimento da RIOPRETOPREV, mapeados e manualizados no âmbito da Coordenadoria Administrativa e da Tecnologia da Informação:
- Manual do Procedimento de Controle de Acesso Lógico aos Sistemas e Bancos de Dados (versão 3.0, de agosto de 2026), que contém, em seu Anexo I, o modelo de Termo de Responsabilidade e Confidencialidade;
- Manual do Procedimento de Controle de Acesso Físico às Dependências, Áreas Sensíveis e Ativos de Informação (versão 3.0, de agosto de 2026);
- Manual do Procedimento de Contingência para Acesso às Cópias de Segurança dos Sistemas Informatizados e dos Bancos de Dados (versão 3.0, de agosto de 2026);
- Manual do Procedimento de Auditoria de Acesso e Rotinas de Recuperação de Desastres (versão 2.0, de agosto de 2026), que contém, em seu Anexo I, o Checklist de Teste de Restauração de Dados.

Considerações finais

Esta Política de Segurança da Informação deverá ser revisada periodicamente, no mínimo a cada 4 (quatro) anos, conforme prescrição do Manual do Pró-Gestão RPPS (Nível IV), ou extraordinariamente, sempre que houver mudança significativa no ambiente tecnológico, normativo ou organizacional da RIOPRETOPREV. A revisão será conduzida pelo CSI/RPP, com deliberação em reunião ordinária ou extraordinária, e a versão atualizada deverá ser publicada na internet da Autarquia.

Sem prejuízo do prazo máximo acima, o CSI/RPP avaliará anualmente a aderência e a efetividade desta Política, registrando a avaliação em ata, de modo a antecipar a necessidade de revisão antes do decurso do prazo quadrienal. Constituem gatilhos de revisão extraordinária, entre outros: incidente de segurança de impacto relevante; alteração legislativa ou regulatória (em especial da LGPD, da Portaria MTP nº 1.467/2022 ou do Manual do Pró-Gestão RPPS); mudança significativa de infraestrutura tecnológica, de fornecedores críticos ou da estrutura organizacional da Autarquia.

Anexo I - Matriz de atendimento ao Manual do Pró-Gestão RPPS, versão 4.1, Nível IV

Requisito do Manual do Pró-Gestão RPPS, versão 4.1 - item 3.1.5, Nível IV	Atendimento no documento	Evidência ou seção correlata	Situação
Existência de Política de Segurança da Informação formalizada, aprovada e aplicável à unidade gestora do RPPS.	A Política define diretrizes corporativas para proteção das informações manipuladas, armazenadas, transmitidas e custodiadas pela RIOPRETOPREV.	Introdução; Objetivos; Princípios; Considerações finais.	Atendido.
Disponibilização e divulgação da Política aos servidores, colaboradores,	O documento prevê publicação no sítio eletrônico da RIOPRETOPREV e	Introdução; Gestão da Segurança da Informação; Termo de Responsabilidade.	Atendido.

RIOPRETOPREV – Regime Próprio de Previdência Social do Município de São José do Rio Preto
Rua General Glicério, 3553 – Centro - CEP 15015-400 - São José do Rio Preto - SP Telefones (17) 3222 7445
E-mail: contato@riopretoprev.sp.gov.br - www.riopretoprev.sp.gov.br

prestadores de serviço e demais interessados.	disponibilização interna, além de ações de divulgação e conscientização.		
Definição de responsabilidades quanto ao uso, guarda, tratamento e proteção das informações.	São estabelecidas responsabilidades para colaboradores, visitantes, gestores, pessoas jurídicas contratadas, clientes, CSI/RPP, Gerência de Cadastro e Sistemas de Informação, Encarregado de Dados e fornecedores.	Responsabilidades; Gestão da Segurança da Informação; Gestão de Fornecedores e Terceiros; Termo de Responsabilidade.	Atendido.
Controle de acesso lógico aos sistemas, bancos de dados, recursos tecnológicos e informações institucionais.	A Política disciplina identificação pessoal, uso de senhas, autenticação multifator, concessão, revisão e revogação imediata de permissões, princípio do menor privilégio, segregação de funções e registros de acesso.	Identificação pessoal; Internet e VPN; Auditoria de Acesso; Assinatura e processo digital; Manual do Procedimento de Controle de Acesso Lógico aos Sistemas e Bancos de Dados (versão 3.0).	Atendido.
Controle de acesso físico às dependências, equipamentos, áreas restritas e ativos de informação.	Há regras para identificação, registro e acompanhamento de visitantes, uso de crachás, restrição de acesso a áreas sensíveis e observância dos controles de prestadores de infraestrutura.	Controle de Acesso Físico; Equipamentos; Visitantes; Manual do Procedimento de Controle de Acesso Físico às Dependências, Áreas Sensíveis e Ativos de Informação (versão 3.0), incluindo o registro obrigatório de ingresso de não servidores em áreas sensíveis.	Atendido.
Classificação das informações e definição de critérios proporcionais de proteção, armazenamento, compartilhamento e descarte.	A Política estabelece níveis de classificação, responsabilidades pela classificação, controles proporcionais ao grau de sigilo e integração com a Tabela de Temporalidade da RIOPRETOPREV.	Classificação da Informação; Arquivos digitalizados; Gestão da Segurança da Informação.	Atendido.
Rotinas de backup, cópias de segurança e	São previstas cópias de segurança em múltiplas camadas, backup de	Backup; Recuperação de Desastres; Manual do Procedimento de	Atendido.

RIOPRETOPREV – Regime Próprio de Previdência Social do Município de São José do Rio Preto
Rua General Glicério, 3553 – Centro - CEP 15015-400 - São José do Rio Preto - SP Telefones (17) 3222 7445
E-mail: contato@riopretoprev.sp.gov.br - www.riopretoprev.sp.gov.br

testes periódicos de restauração.	sistemas críticos, armazenamento seguro, testes semestrais e simulação anual de recuperação de desastres.	Contingência para Acesso às Cópias de Segurança dos Sistemas Informatizados e dos Bancos de Dados (versão 3.0); Checklist de Teste de Restauração de Dados (Anexo I do Manual de Auditoria de Acesso e Rotinas de Recuperação de Desastres, versão 2.0).	
Procedimentos de recuperação de desastres e continuidade mínima dos serviços críticos.	A Política contempla análise de riscos, backup regular, procedimentos de recuperação, testes periódicos, identificação de pessoal-chave, comunicação de emergência e atualização contínua.	Recuperação de Desastres; Backup; Gestão de Riscos de Segurança da Informação; Manual do Procedimento de Auditoria de Acesso e Rotinas de Recuperação de Desastres (versão 2.0), com metas de RTO e RPO por sistema.	Atendido.
Auditoria de acesso lógico, rastreabilidade, manutenção de logs e verificação periódica de permissões.	O documento prevê logs, revisão semestral de permissões, revogação imediata de acesso em caso de desligamento, remanejamento ou incidente, monitoramento, testes de vulnerabilidade e capacitação dos usuários sobre práticas seguras de acesso.	Auditoria de Acesso, com prazos objetivos de retenção de logs; Identificação pessoal; Proteção de Endpoint e Antivírus; Manual do Procedimento de Auditoria de Acesso e Rotinas de Recuperação de Desastres (versão 2.0).	Atendido.
Gestão de incidentes de segurança da informação, incluindo registro, comunicação, tratamento e aprendizado institucional.	A Política define incidente, canais de comunicação, classificação de gravidade, contenção, investigação, registro, comunicação à Diretoria, à ANPD e aos titulares quando cabível, além de relatório para melhoria contínua.	Princípios; Resposta a Incidentes de Segurança da Informação; Da Política de Privacidade de Dados Pessoais.	Atendido.
Proteção de dados pessoais e observância	São disciplinados o papel do Encarregado	Da Política de Privacidade de Dados	Atendido.

RIOPRETOPREV – Regime Próprio de Previdência Social do Município de São José do Rio Preto
Rua General Glicério, 3553 – Centro - CEP 15015-400 - São José do Rio Preto - SP Telefones (17) 3222 7445
E-mail: contato@riopretoprev.sp.gov.br - www.riopretoprev.sp.gov.br

da LGPD nas atividades do RPPS.	de Dados, a Política de Privacidade, o Registro das Operações de Tratamento de Dados Pessoais, a comunicação de incidentes e a proteção de informações pessoais e sensíveis.	Pessoais; Classificação da Informação; Resposta a Incidentes de Segurança da Informação.	
Gestão de riscos de segurança da informação, com identificação, avaliação, tratamento e monitoramento dos riscos.	A Política prevê processo contínuo de gestão de riscos, matriz de probabilidade e impacto, níveis de criticidade, estratégias de tratamento e revisão periódica.	Gestão de Riscos de Segurança da Informação; Inventário de Ativos de Informação; Recuperação de Desastres.	Atendido.
Inventário de ativos de informação e indicação de responsáveis pelos ativos.	O documento determina a manutenção de inventário atualizado de sistemas, bases de dados, documentos, equipamentos, infraestrutura e serviços de terceiros, com identificação de responsável, classificação e custodiante.	Inventário de Ativos de Informação; Classificação da Informação.	Atendido.
Gestão de fornecedores e terceiros que acessem, armazenem ou tratem informações do RPPS.	São exigidas cláusulas contratuais de segurança da informação, confidencialidade, comunicação de incidentes, direito de auditoria, verificação prévia de requisitos mínimos e devolução ou eliminação segura dos dados ao final do contrato.	Pessoas jurídicas contratadas; Gestão de Fornecedores e Terceiros.	Atendido.
Conscientização, capacitação e orientação dos usuários sobre segurança da informação.	A Política prevê divulgação ampla, ações de conscientização, treinamento de usuários, boas práticas de uso de recursos tecnológicos, prevenção contra phishing, engenharia	Gestão da Segurança da Informação; Correio eletrônico; Auditoria de Acesso; Uso de Inteligência Artificial; Comportamento esperado.	Atendido.

RIOPRETOPREV – Regime Próprio de Previdência Social do Município de São José do Rio Preto
Rua General Glicério, 3553 – Centro - CEP 15015-400 - São José do Rio Preto - SP Telefones (17) 3222 7445
E-mail: contato@riopretoprev.sp.gov.br - www.riopretoprev.sp.gov.br

	social e uso responsável de IA.		
Revisão periódica da Política de Segurança da Informação em prazo compatível com o Nível IV.	A Política prevê revisão mínima a cada 4 anos, avaliação anual de aderência e revisão extraordinária diante de incidentes relevantes, alterações normativas, mudanças tecnológicas, fornecedores críticos ou estrutura organizacional.	Considerações finais.	Atendido.
Manutenção de evidências documentais para auditoria, certificação, supervisão e melhoria contínua.	O documento prevê registros em processo digital, relatórios de incidentes, atas do CSI/RPP, matriz de riscos, inventário de ativos, registros de uso de IA, termos de responsabilidade e relatórios de testes de restauração.	Resposta a Incidentes de Segurança da Informação; Gestão de Riscos; Termo de Responsabilidade; Backup; Uso de Inteligência Artificial.	Atendido, condicionado à manutenção atualizada das evidências.

RIOPRETOPREV – Regime Próprio de Previdência Social do Município de São José do Rio Preto
Rua General Glicério, 3553 – Centro - CEP 15015-400 - São José do Rio Preto - SP Telefones (17) 3222 7445
E-mail: contato@riopretoprev.sp.gov.br - www.riopretoprev.sp.gov.br