POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DA RIOPRETOPREV

Versão 3.1, de 18 de dezembro de 2023

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 1ª Reunião Extraordinária da Comissão de Segurança da Informação/CSI – Realizada em 18/12/2023. Documento elaborado em atendimento ao disposto no item 3.1.5 do Manual do Pró-Gestão RPPS.

Comissão de Segurança da Informação – CSI/RPP

riopretoprev@riopreto.sp.gov.br

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

Edinho Araújo
Prefeito Municipal

Jair Moretti
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

Sumário

1. Introdução

No presente documento são estabelecidas as diretrizes corporativas no âmbito da segurança das informações manipuladas e transitadas pela autarquia.

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, garantindo que os mesmos sempre possam estar disponíveis a quem necessita e a quem é de direito.

A cada vez que uma informação é manipulada, a mesma está sujeita a erros, sejam causados pelas máquinas que a manipulam quanto pelos seres humanos. Desta forma, é importante que hajam diretrizes visando a minimização desse tipo de problema, com o principal intuito de proteger a informação corporativa.

Este documento está disponível na intranet da autarquia, aberto para consultas.

2. Objetivos

O objetivo da PSI apresentada aqui é instruir os servidores da RIOPRETOPREV e demais pessoas interessadas com procedimentos a serem adotados para que se tenha uma maior segurança dos dados.

A ideia é alertar aos 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.

3. 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, sistemas e informações são utilizados pelos colaboradores para a realização das atividades profissionais. O uso pessoal dos recursos é permitido desde que não prejudique o desempenho dos sistemas e serviços e estejam plenamente de acordo com o estabelecido no Código de Ética da instituição.

Qualquer incidente que possa afetar a segurança da informação deverá ser comunicado à gerência de Cadastro e Sistemas de Informação para que as devidas providências sejam tomadas.

4. Responsabilidades

i. 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 da qual têm conhecimento e/ou que manipulam em razão do seu serviço, devendo privar pela sua proteção.

ii. Visitantes

Qualquer pessoa que venha até a sede da autarquia é considerada visitante. A mesma também está 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 também 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.

iii. Gestores

Qualquer pessoa que possua um colaborador, equipe ou processo sob sua supervisão é considerado gestor. O gestor, além de responsável pelos seus atos, também responde pelos atos de seus diretos, devendo esse zelar pela proteção da informação manipulada 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 a mesma não seja infringida.

iv. 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 a que tiver conhecimento, seja mediante contrato ou

solicitação de serviço. As pessoas jurídicas também são responsáveis pelos prestadores de serviços enviados, respondendo solidariamente a qualquer incidente ocorrido com os mesmos.

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.

v. Clientes

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

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.

5. 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;

- 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 superior a 10MB;
    - 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.

6. Comunicador instantâneo

Atualmente, o comunicador instantâneo oficial da RIOPRETOPREV é o Spark®, conforme configuração realizada pela empresa Empro Tecnologia e Informação (Empro). O uso de outros softwares da mesma natureza é permitido, desde que seja respeitado o Código de Ética da entidade e que se mostre mais eficiente ou com maior utilidade que o Spark®.

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 para envio de mensagens sem autorização explícita e sem identificar-se adequadamente;
- Enviar mensagens difamatórias, ofensivas, preconceituosas, obscenas, caluniosas ou que tenham fins de propaganda política;
- Utilizar de avatares ou frases de status que sejam difamatórias, ofensivas, preconceituosas, obscenas, caluniosas ou que tenham fins de propaganda política.

Caso haja a necessidade de realização de videoconferência com compartilhamento de tela, o usuário responsável pela tela compartilhada deve garantir que nenhuma informação, além da necessária, seja transmitida. O mesmo também deve alertar ao destinatário sobre as consequências do uso indevido das informações que receber.

O conteúdo textual de toda comunicação realizada via Spark® é armazenado nos servidores da Empro, podendo ser consultado pela ferramenta de Log do software, dentro do período de 1 (um) ano. O servidor que utilizar outro comunicador, especialmente para contato externo, deve se preocupar em manter o histórico das conversas ao menos pelo mesmo período.

7. 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 monitoria e 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. O mesmo se aplica 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 usar a conexão wifi disponibilizada pela Empro, desde que complacentemente com as normas do Código de Ética e 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 é possível a transferência de arquivos entre os computadores das redes distintas, devem ser observadas as mesmas regras dispostas na seção 12, tomando todas as precauções possíveis para que as informações usadas no trabalho não sejam disponibilizadas a qualquer outra pessoa não competente que possa ter acesso ao mesmo computador do usuário. Assim, recomenda-se que a referida transferência de arquivos seja realizada apenas quando for imprescindível para o trabalho realizado.

Também é importante salientar que, mesmo em trabalho remoto, o servidor está sujeito à totalidade desta Política de Segurança das Informações.

8. Servidor de arquivos

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 do mesmo;
- Fraudar, de qualquer forma, as informações dos arquivos;
- Instalar ou armazenar programas sem o conhecimento da área de TI;
- 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 área de TI para avaliação, desde que haja justificativa plausível.

9. Identificação pessoal

Os dispositivos de identificação (o que inclui CPF's e assinadores digitais) e senhas protegem a identidade do colaborador usuário, evitando e prevenindo que uma pessoa se faça passar por outra perante a RIOPRETOPREV e/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.

Mesmo que o sistema utilizado permita o uso de senhas simples, as seguintes regras devem ser seguidas para a confecção da senha, de forma a tornar mais difícil uma eventual tentativa de fraude:

- 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.

Caso haja esquecimento de senha, ou qualquer outro problema de acesso, o colaborador deverá entrar em contato pessoalmente com a área responsável.

10.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, o mesmo deve ser comunicado à área de TI para que a manutenção seja providenciada.

Caso existam informações que necessitem ser armazenadas no HD da máquina alocado ao usuário, este deve fazê-lo na área protegida do usuário, preferencialmente no diretório "Documentos", pois isto evita que outros usuários que venham a utilizar o mesmo equipamento tenha acesso a tais dados.

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.

11. 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-dia:

- Retirada dos papéis da impressora: toda vez que alguém enviar um documento para impressão, o mesmo deve ser retirado imediatamente após o término da mesma, de forma a evitar que ele 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 aqueles sensíveis e/ou que envolvem 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.

12.Dispositivos móveis

Considera-se dispositivo móvel qualquer aparelho que tenha atribuições de mobilidade, tal como: notebook, smartphone, *pendrive* e DVD's.

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 na seção de uso da internet devem ser respeitadas, seja qual for o ponto de acesso, de acordo com o exposto na seção 7 deste documento.

13.Backup (cópia de segurança)

A segurança e integridade dos dados são prioridades fundamentais em nossa infraestrutura de tecnologia. Para assegurar essa proteção, rotinas de backup automáticas foram implementadas em diferentes sistemas críticos, cada um gerenciado por empresas especializadas em suas respectivas áreas.

No que diz respeito aos arquivos armazenados no servidor central, sob responsabilidade da Empro, foi adotada uma abordagem proativa, com rotinas automáticas de backup que garantem que todos os diretórios e arquivos sejam copiados regularmente para um repositório seguro na nuvem (cloud backup). Essa prática elimina a necessidade de intervenção humana, proporcionando uma camada adicional de segurança contra possíveis falhas de hardware.

Os e-mails, também gerenciados pela Empro, são submetidos a um sistema de backup automático altamente eficiente. As informações críticas contidas nas comunicações eletrônicas são preservadas por meio de processos automáticos que ocorrem várias vezes ao dia. Isso não apenas garante a continuidade das operações, mas também possibilita a recuperação de dados históricos em caso de necessidade.

No âmbito do sistema previdenciário e de folha de pagamento, a empresa Aspprev assume a gestão desses dados sensíveis. Implementamos um protocolo de backup automático robusto que, de forma programada e sem intervenção manual, realiza cópias regulares da base de dados. Essa prática é essencial para assegurar a integridade das informações relacionadas às obrigações previdenciárias e folha de pagamento.

Para o sistema de processos digitais, gerenciado pela empresa 1Doc, adotamos uma abordagem semelhante. Rotinas automáticas de backup são configuradas para preservar os dados relacionados aos processos digitais. Essa estratégia não apenas protege informações cruciais, mas também permite uma recuperação eficiente em casos de eventualidades.

Essas práticas de backup automático são essenciais para garantir a continuidade dos negócios, preservar a integridade dos dados e proporcionar uma resposta eficaz em situações adversas. Cada empresa parceira desempenha um papel crucial na manutenção dessas operações críticas, reforçando nosso compromisso com a segurança e confiabilidade dos sistemas em uso.

14.Auditoria de Acesso

A auditoria de acesso é um componente crucial na gestão da segurança da informação, garantindo que os sistemas e dados estejam protegidos contra acessos não autorizados. A seguir, apresentamos um conjunto de procedimentos essenciais aplicados junto às empresas fornecedoras dos sistemas:

a) Definição de Políticas de Acesso

Estabelecemos políticas claras de acesso, incluindo a determinação de quem tem permissão para acessar quais dados e sistemas, com base nas funções e responsabilidades de cada usuário.

b) Revisão Regular de Permissões

Realizamos revisões periódicas das permissões de acesso. Certificamo-nos de que as credenciais concedidas aos usuários estejam alinhadas com suas responsabilidades atuais, evitando o acúmulo desnecessário de privilégios.

c) Monitoramento em Tempo Real

Implementamos ferramentas de monitoramento em tempo real para identificar atividades suspeitas. Isso inclui tentativas de acesso não autorizado, alterações nas permissões e padrões de comportamento fora do comum.

d) Registro de Auditoria

Mantemos registros detalhados de todas as atividades de acesso. Esses registros são armazenados de forma segura e revisados regularmente para detectar possíveis violações de segurança.

e) Testes de Penetração

Realizamos testes de penetração regularmente para identificar vulnerabilidades nos sistemas de acesso. Isso ajuda a garantir que as medidas de segurança estejam efetivas contra ameaças externas e internas.

f) Treinamento de Usuários

Fornecemos treinamento contínuo aos usuários sobre práticas seguras de acesso. Isso inclui a importância de senhas robustas, autenticação de dois fatores e a conscientização sobre possíveis ataques de phishing.

15. Recuperação de Desastres

A recuperação de desastres é uma parte crítica do plano de continuidade de negócios, visando minimizar o impacto de eventos adversos. Abaixo, destacamos as principais rotinas implementadas com o auxílio da empresa Empro Tecnologia e Informação (Empro):

a) Análise de Riscos

Iniciamos com uma análise abrangente de riscos para identificar potenciais ameaças que podem afetar os sistemas e operações. Isso inclui desastres naturais, falhas de hardware, ataques cibernéticos e outros eventos imprevistos.

b) Backup Regular

Implementamos um plano de backup regular e automatizado para todos os dados críticos. Esses backups são armazenados de forma segura em locais geograficamente distintos para garantir a disponibilidade dos dados em caso de perda.

c) Procedimentos de Recuperação

Desenvolvemos procedimentos detalhados de recuperação para cada sistema e conjunto de dados. Isso inclui a sequência de passos para restaurar sistemas, aplicativos e dados essenciais de backup.

d) Testes Periódicos

Realizamos testes regulares dos procedimentos de recuperação de desastres para garantir que possam ser executados efetivamente quando necessário. Isso inclui simulações de desastres para avaliar a eficácia do plano.

e) Identificação de Pessoal-Chave

Mantemos uma lista atualizada de pessoal-chave responsável pela execução do plano de recuperação. Certificamo-nos de que cada membro da equipe esteja familiarizado com suas responsabilidades durante uma situação de desastre.

f) Comunicação de Emergência

Estabelecemos protocolos de comunicação de emergência para garantir uma comunicação rápida e eficaz entre os membros da equipe durante um evento de recuperação de desastres.

g) Armazenamento de Documentação

Documentamos todas as informações relevantes, incluindo configurações de sistemas, senhas, procedimentos de recuperação e detalhes de

contato de fornecedores. Armazenamos esses documentos de forma segura e de fácil acesso.

h) Atualização Contínua

Revisamos e atualizamos regularmente o plano de recuperação de desastres para refletir mudanças na infraestrutura de TI, na equipe e nas ameaças potenciais.

16.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 9, 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 área de TI 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 pelo seu cuidado, bem como pela integridade de todas as informações ali contidas, seja de processos de próprio interesse ou de processos de terceiros a que venha a ter conhecimento.

17.Arquivos digitalizados

A digitalização de documentos para a Riopretoprev deve seguir o disposto no Decreto Federal nº 10.278, de 18 março de 2020, considerando que a tabela de temporariedade de guarda e classificação de documentos será publicada mediante Portaria específica.

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 mesmo, 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 equipe de TI é a responsável por indicar e instalar eventual software substituto. Os parâmetros utilizados para tal devem ser configurados pelo time de TI no computador do usuário.

Os dados e metadados do arquivo gerado são responsabilidade do digitalizador e do detentor do documento. Tais informações devem ser cadastradas através de software próprio para edição de metadados, a ser indicado pela equipe de TI. 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 diretórios do servidor, visto que tanto o arquivo quanto seus metadados podem possuir informações sigilosas e/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.

18. Da Política de Privacidade de Dados Pessoais

A RIOPRETOPREV deve editar documento conhecido como "Política de Privacidade". Este documento detalhará os seguintes aspectos:

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.

19.Considerações finais

Espera-se que a PSI aqui apresentada possa guiar as ações de todos os usuários da RIOPRETOPREV de forma a zelar, da melhor maneira possível, pelas informações da autarquia.

Qualquer dano às informações é muito prejudicial a todos que necessitam dela, então é muito importante que todos estejam engajados em protegê-la.

Este documento deverá ser revisado a cada dois anos e poderá ser alterado no futuro para contemplar fatos e tecnologias não previstas no momento. Neste caso, haverá devida comunicação aos usuários.