PREVICRATO

FUNDO DE PREVIDÊNCIA SOCIAL DO MUNICÍPIO DO CRATO - CE

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO
2023/2024

undo Previdência Social do Município do Crato-CE - PREVICRATO
Av. Maildes de Siqueira, S/N, Cep: 63104-128
CNPJ: 12.903.772/0001-12
previcrato@gmail.com
www.previcrato.com.br

José Ailton de Sousa Brasil
Prefeito do Município do Crato

André Barreto Esmeraldo
Vice-Prefeito do Município do Crato

Antonio de Pádua Amador de Albuquerque
Presidente RPPS PREVICRATO

Ingride Feitosa Siebra
Coordenadora Especial de Benefícios do PREVICRATO

Paulo Welber Bezerra Bastos
Coordenador Especial Financeiro do PREVICRATO

Sandra Verônica Siqueira
Coordenadora Especial Administrativa do PREVICRATO

Heládio Teles Duarte
Coordenador Especial de Perícias Médicas do PREVICRATO

Gilvânia Olimpio Gomes de Mattos
Coordenadora Especial de Relações Institucionais do PREVICRATO

Sumário

1. Introdução

Esta Política de Segurança da Informação (PSI) trará um conjunto de regras gerais, tendo como objetivos principais: estabelecer os procedimentos para a correta utilização dos ativos tecnológicos, evitar riscos de falhas e danos, promover a conscientização indicando a responsabilidade de cada servidor ou prestador de serviço quanto à segurança das informações, externar regras normativas quanto ao uso da internet, do correio eletrônico, dos computadores e outros recursos tecnológicos do Regime Próprio de Previdência Social (RPPS), além de evidenciar os procedimentos de contingência, salientando as medidas adequadas a serem realizadas como, cópias de segurança e controles de acessos físicos e lógicos, por exemplo.

A política será o principal norteador do Fundo de Previdência Social do Município do Crato-CE - PREVICRATO, devendo ser cumprida por todos os servidores e prestadores de serviço para fins da segurança da informação, visando assegurar a proteção dos dados, documentos e informações diversas sobre responsabilidade do RPPS respeitando os princípios fundamentais: da confiabilidade, garantindo com que determinadas informações sejam disponíveis apenas para as pessoas autorizadas; da integridade, assegurando a exatidão das informações e dos processos; e por fim atendendo o princípio da disponibilidade, priorizando a transparência e fortalecendo a gestão, garantindo com que os interessados, desde que autorizados, tenham acesso às informações requeridas e pertinentes de maneira rápida, atendendo as suas demandas de maneira tempestiva.

2. Responsabilidades

Todas as pessoas que possuem algum contato ou que precisem ter acesso às informações internas não divulgadas no site do PREVICRATO, necessitam respeitar e ter ciência de suas responsabilidades, além de demonstrar zelo pelas informações, cujos detalhes serão expostos a seguir. Assim, cuidar adequadamente dos equipamentos tecnológicos, garantir a sua integridade e o seu perfeito funcionamento, responsabilizar-se por transferir para o servidor designado as informações do computador e a tarefa de possuir cópias de segurança dos seus documentos de trabalho são as principais responsabilidades dos servidores, da Coordenadoria Executiva e dos prestadores de serviço do PREVICRATO.

Aposentados, Pensionistas e Visitantes do RPPS

Qualquer pessoa que venha a sede do PREVICRATO ou que realize uma solicitação de atendimento por meio digital, sejam elas: seus aposentados, pensionistas

ou qualquer indivíduo, os mesmos estão sujeitos à política de segurança da informação, devendo o mesmo se identificar pessoalmente ou por meio digital, informando no mínimo seu nome ede preferência demonstrando seu documento original válido com foto.

Caso o objetivo do visitante seja solicitar documentos específicos perante o RPPS, outros dados e documentos poderão ser solicitados. Os visitantes devem ser supervisionados pela pessoa visitada, a qual é responsável pelos dados aos quais aquele tem acesso e também pelos equipamentos utilizados. Além disso, o visitado tem a responsabilidade de avisar ao visitante sobre as normas de PSI do PREVICRATO.

Servidores

Para efeito dessa PSI, serão chamados de servidores, qualquer pessoa que possua um vínculo direto com o PREVICRATO, seja por tempo determinado ou indeterminado, podendo ser: os servidores efetivos, os servidores comissionados e/ou os estagiários.

Representantes dos Órgãos Colegiados

Já os representantes dos órgãos colegiados são os membros titulares e suplentes do Conselho Administrativo e Fiscal e do Comitê de Investimentos, essas pessoas possuem a responsabilidade sobre as informações que têm acesso, conhecimento e/ou manipulam em razão das suas atribuições devendo zelar pela sua proteção.

Coordenadoria Executiva

Segundo a Lei Municipal n° 2.630/2010 e Lei Municipal n° 3.804/2021que dispõe sobre a criação do PREVICRATO é estabelecido que o mesmo será constituído principalmente por seu Presidente, Coordenação Administrativa, Coordenação Financeira, Coordenação de Benefícios, Coordenação Institucional e Coordenanção de Perícias Médicas, em conjunto com o Conselho Administrativo e Fiscal e o Comitê de Investimentos, devendo zelar pela proteção das informações que foram passadas pela sua equipe.

O Presidente, e os demais servidores do PREVICRATO devem ser verdadeiros modelos de conduta e boas práticas para a equipe, orientando-os e fiscalizando-os

constantemente para que incidentes relacionados à PSI não ocorram. Eles também deverão adaptar os processos e procedimentos sobre sua responsabilidade à política, cuidando para que a mesma não seja infringida, evitando maiores problemas.

Prestadores de Serviço

Qualquer pessoa jurídica que seja, ou venha a ser contratada para prestação de serviços ao PREVICRATO, é responsável por cuidar das informações do RPPS a que tiver conhecimento. As pessoas jurídicas também são responsáveis diretamente pelos seus respectivos funcionários que representam a empresa, respondendo solidariamente a qualquer incidente ocorrido pelos mesmos.

A empresa que possuir banco de dados com informações de propriedade do PREVICRATO deve zelar pela sua proteção, e respeitar os princípios da segurança da informação expostos da confidencialidade, integridade ou disponibilidade dos dados, comentados anteriormente. Os dados fornecidos pelo PREVICRATO as empresas não devem ser divulgados ou repassados a terceiros sem que ocorra uma autorização prévia.

3. Regras e Formas de Uso

Equipamentos Tecnológicos

O servidor é responsável por cada equipamento que usar, sendo primordial zelar por sua conservação. Caso ocorra qualquer problema com os equipamentos, a área de TI deverá ser acionada e providenciar tempestivamente a manutenção do equipamento. O acesso aos computadores, sistemas e arquivos da rede do PREVICRATO será feito através de credenciais de acesso de uso pessoal e visando o melhor acompanhamento do que cada usuário acessa.

Desta forma, o computador deverá ser bloqueado quando o usuário se ausentar do seu setor, mesmo que por breve período de tempo, se o usuário tiver que se ausentar por tempo indeterminado deverá desligar o mesmo. Apenas a equipe de TI com seu usuário de administrador está autorizada à instalar softwares de qualquer tipo nos computadores, devendo os servidores solicitarem uma permissão especifica com a devida justificativa para instalação.

Internet

O servido deverá usar a internet exclusivamente para assuntos profissionais, sendo vedado:

- Acessar sites com conteúdos divergentes com os interesses do RPPS;
- Utilização de redes sociais;

- Acessar sites com conteúdos ofensivos, ilegais, impróprios, pornográficos e comércios eletrônicos;
- Acessar sites de estrutura duvidosa que ofereçam risco à segurança da informação ou que possuam ferramentas que visem prejudicar a segurança dos dispositivos tecnológicos;
- o Uso e instalação de jogos ou de download de arquivos que comprometam o tráfego da rede (vídeos, imagens, músicas, etc.), para fins particulares;
- Utilizar computadores públicos ou compartilhados, como terminais em aeroportos e shopping centers para acessar documentos e sistemas exclusivos do PREVICRATO.

Aconselha-se somente enviar informações e dados pessoais através de sites seguros, para identificar que o site é seguro verifique se o seu endereço (URL) é iniciado por HTTPS:// ou se no navegador é exibido à figura de um cadeado fechado.

O acesso aos sites de instituições financeiras e públicas deverão ser feitos digitando o link de acesso diretamente no navegador, nunca acessando através do clique em outros sites correlatos, propagadas ou por e-mails recebidos, evitando que sites fraudulentos sejam acessados.

Correio Eletrônico

O correio eletrônico é utilizado para fins corporativos e relacionado às atribuições dos servidores, ou seja, deverá ser usado com integridade e coerência, não podendo ser utilizado para fins particulares nem para envio de spams, propaganda, conteúdo impróprio, difamatório, calunioso ou que prejudique a imagem do RPPS, deixando a mesma vulnerável a ações civis ou criminais.

É vedado também:

- Enviar mensagens usando nome de usuário de outra pessoa ou endereço eletrônico que não esteja autorizado a usar;

- 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;
- Abrir e-mails de origem duvidosa, ou que julgar não pertinentes ao seu trabalho no RPPS, incluindo anexos;
- Divulgar seu e-mail corporativo para sites e serviços de internet não seguros.

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

Acesso aos Arquivos da Rede

Os documentos do PREVICRATO devem ser salvos na rede, nas pastas das respectivas Coordenadorias de maneira organizada e linear, na qual serão realizados backups periódicos, objetivando criar cópias em outros lugares segregados ao de origem, como o HD externo do PREVICRATO e pastas na nuvem em sites confiáveis.

Os coordenadores de cada setor são os responsáveis por determinar a relação de servidores que têm acesso aos documentos pertinentes à Coordenadoria sob sua responsabilidade. O acesso é controlado mediante autenticação do usuário com login e senha pessoal, registrados e liberados pela área de Tecnologia da Informação (TI) da Prefeitura Municipal do Crato.

É vedado utilizar a pasta da rede para:

- Armazenar arquivos que não tenham relação com o trabalho realizado, especialmente filmes 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;
- Armazenar conteúdo protegido por direitos autorais ou patentes.

Acesso Remoto

O acesso remoto de terceiros à rede do PREVICRATO será realizado através de programas específicos para esse fim, que tenham um nível de segurança das informações. Precisará ser permitido mediante autorização prévia do Presidente Executivo do PREVICRATO, para atender necessidades especificas e deverá ser acompanhado por um servido do RPPS, o processo será realizado respeitando os

princípios da integridade e confidencialidade.

Os técnicos de TI da Prefeitura Municipal do Crato, ou outros administradores da rede, poderão fazer o acesso remoto ao computador, sem necessidade de autorização prévia do Presidente Executivo, para manutenção ou instalação de programas necessários para as atribuições do servido.

Assim, as pessoas que tiverem acesso as informações devem mantê-las sobre sigilo e comunicar imediatamente aos servidores do PREVICRATO qualquer situação adversa que tenha ocorrido e colocado em risco o acesso ao ambiente de rede do RPPS de Crato.

Acesso Através de VPN

Considerando a possibilidade de regime híbrido de trabalho, alternando entre presencial e remota, deverá ser solicitado por cada servidor apto a trabalhar nesses regimes de trabalho, desde que autorizado pelo Presidente Executivo do RPPS, um acesso remoto à rede interna e, consequentemente, aos dados necessários e ao computador de trabalho mediante VPN (*Virtual Private Network*). Uma vez conectado através dessa VPN, o servidor estará sujeito às mesmas regras de quando utiliza a rede interna presencialmente, estando sujeito a esta PSI

As senhas e configurações da rede VPN são atreladas ao usuário e senha cadastrados na rede, sendo, portanto, pessoais e intransferíveis. Sendo então de responsabilidade dos usuários manter a sua confidencialidade para evitar acessos de pessoas não autorizadas.

4. Procedimentos de Contingência

São estabelecidos procedimentos para o controle e tratamento de incidentes com foco na redução dos impactos encontrados e causados por desastres ocasionais nos serviços de tecnologia da informação. Primeiramente quando um problema é exposto deve ser realizado seu mapeamento para saber o seu nível de incidência e consequentemente o mesmo será direcionado para que a área de TI da prefeitura consiga ser mais especifica e assertiva na resolução do problema, reduzindo o tempo de indisponibilidade dos serviços e evitando maiores danos e prejuízos em razão do incidente.

Níveis de Incidência

- Nível 1 – Hipótese acidental que pode ser controlada pelo Setor de Material e Patrimônio do PREVICRATO e que não afeta o andamento do trabalho do servido. Ex.: Problemas com periféricos do computador.
-
- Nível 2 - Hipótese acidental que impede a utilização do equipamento ou sistema e acaba impedindo a continuação do trabalho do servido.

  Ex: Problema com o funcionamento do computador ou ainda sistema offline impedindo o uso do mesmo.

- Nível 3 – Hipótese acidental que impede o uso de sistemas ou equipamentos de todo o PREVICRATO, impedindo o desenvolvimento do trabalho de todos os servidores.
  Ex: Falha de conexão com a internet, queda da rede e queda de energia.

Principais Riscos

- Interrupção de energia elétrica: ocasionado por fatores externos, como falta de energia elétrica na localidade e por fatores internos, como curto-circuito, incêndio e infiltrações;

- Indisponibilidade de rede/ circuitos: originado pelo rompimento de cabeamento decorrente de execuções de obras internas, desastres ou acidentes;

- Falha humana: acidente ao manusear equipamentos;

- Falha de hardware: falha que necessite reposição de peças ou reparos;

- Ataques internos: ataques intencionais causados pelos próprios servidores;

- Ataques cibernéticos: ataque virtual que compromete o desempenho, os dados ou configuração dos serviços essenciais;

- Desastres Naturais/ Incêndios: Fenômenos externos com interferência de pessoas ou de forma natural.

Principais Procedimentos de Contingência

Cópias de Segurança

Backup é uma cópia de segurança que tem o objetivo de resguardar o PREVICRATO de uma ocasional perda de arquivos originais, seja por ações despropositadas ou ainda pelo mau funcionamento dos sistemas. O backup deverá ser feito em local segregado e seguro, através de meios físicos, como HD externo ou pendrive e meios virtuais, armazenamento em nuvens ou e-mails.

Desta forma, cada Coordenador deverá ser responsável por fazer o backup dos documentos pertinentes à Coordenadoria sob sua responsabilidade, podendo delegar a responsabilidade para um servido e acompanhar a tarefa. O procedimento deverá ser realizado periodicamente, de forma a prevenir qualquer perda de informação em caso de falha do equipamento que utiliza.

Será exposto como anexo I desta política a manualização e o mapeamento do processo de backup realizado pelo PREVICRATO.

Controle de Acesso Físico e Lógico

O controle de acesso aos dispositivos tecnológicos é realizado de maneira constante, tendo em vista que todos os computadores e notebooks alocados ao PREVICRATO são acessados mediante autenticação do usuário com login e senha pessoal, registrados e liberados pela área de Tecnologia da Informação (TI) da Prefeitura Municipal do Crato. O processo detalhado para criação do login e da senha do servido ou prestador de serviço estará exposto no anexo II desta política.

Apenas após o registro efetivo do colaborar e a criação do usuário é que o mesmo terá acesso compartilhado aos arquivos de rede e também ocorrerá sua liberação para instalação e consequente uso de sistemas internos fornecidos pela prefeitura, além da disponibilização para acesso à internet e a maioria dos demais aplicativos de uso comum na internet. A senha para acesso aos dispositivos do PREVICRATO sempre deverão respeitar os critérios estabelecidos de segurança e não podem ser divulgadas a terceiros.

O controle de acesso físico também é realizado na recepção do RPPS visando promover e manter a proteção das repartições públicas e zelar pela segurança dos servidores municipais quando no exercício de suas atribuições.

5. Considerações Finais

Espera-se que a PSI apresentada possa guiar as ações de todos que fazem parte de alguma forma do PREVICRATO, zelando da melhor maneira possível, pelas informações do RPPS, seguindo os princípios da confiabilidade, integridade e disponibilidade, sempre com a participação de todos os envolvidos.

A manutenção da base de dados atualizada e segura é um grande passo para a boa gestão previdenciária, portanto este documento está em constante evolução para contemplar fatos e tecnologias não previstas no momento, mantendo o mesmo nível de segurança das informações.

Antonio de Pádua Amador de Albuquerque
Presidente do RPPS PREVICRATO
Port. nº 0107019/2021 - GP