



DECRETO Nº 102/2023

Aprova a Política de Segurança da Informação do RPPS do Município de Restinga Sêca.

PAULO RICARDO SALERNO, PREFEITO MUNICIPAL DE RESTINGA SÊCA, no uso de suas atribuições legais e de conformidade com a Lei Municipal nº 2.351/2007, de 15 de outubro de 2007, e alterações,

DECRETA:

Art. 1º Fica aprovada a Política de Segurança da Informação do Regime Próprio de Previdência Social – RPPS do Município de Restinga Sêca, passando a integrar este Decreto.

Art. 2º Este Decreto entra em vigor na data de sua publicação.

GABINETE DO PREFEITO MUNICIPAL, aos 26 de dezembro de 2023.

Registre-se e publique-se.

JOÃO IRAJÁ ROSA DA SILVA
Secretário de Administração

PAULO RICARDO SALERNO
Prefeito Municipal



POLÍTICA DA SEGURANÇA DA INFORMAÇÃO

Restinga Sêca, 18 de dezembro de 2023



ÍNDICE

CAPÍTULO I	DOS OBJETIVOS DA PSI
CAPÍTULO II	DAS APLICAÇÕES DA PSI
CAPÍTULO III	DAS RESPONSABILIDADES ESPECÍFICAS
CAPÍTULO IV	DO MONITORAMENTO E DA AUDITORIA DO AMBIENTE
CAPÍTULO V	DO CORREIO ELETRÔNICO
CAPÍTULO VI	DA INTERNET
CAPÍTULO VII	DOS COMPUTADORES E OUTROS DISPOSITIVOS
CAPÍTULO VIII	DA IDENTIFICAÇÃO E CONTROLE DE ACESSO
CAPÍTULO IX	DOS PROCEDIMENTOS DE CONTINGÊNCIA
CAPÍTULO X	DAS DISPOSIÇÕES FINAIS



CAPÍTULO I DOS OBJETIVOS DA PSI

Art. 1º A Política de Segurança da Informação, também referida como PSI, é o documento que orienta e estabelece as diretrizes corporativas do RPPS para a proteção dos ativos de informação e a responsabilidade legal para todos os usuários. Deve, portanto, ser cumprida e aplicada em todas as áreas do Fundo e por todos os colaboradores e prestadores de serviço que tenham acesso às informações de propriedade do RPPS.

Art. 2º Constitui objetivo da PSI:

I - estabelecer diretrizes que permitam aos colaboradores e fornecedores do RPPS seguirem padrões de comportamento relacionados à segurança da informação adequados às necessidades de negócio e de proteção legal do RPPS e do indivíduo;

II - nortear a definição de normas e procedimentos específicos de segurança da informação, bem como a implementação de controles e processos para seu atendimento;

III - preservar as informações do RPPS quanto à:

a) Integridade: garantia de que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais;

b) Confidencialidade: garantia de que o acesso à informação seja obtido somente por pessoas autorizadas;

c) Disponibilidade: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

CAPÍTULO II DAS APLICAÇÕES DA PSI

Art. 3º As diretrizes aqui estabelecidas deverão ser seguidas por todos os colaboradores, bem como os prestadores de serviços, e se aplicam à informação em qualquer meio ou suporte.

Parágrafo único. É obrigação de cada colaborador se manter atualizado em relação a esta PSI e aos procedimentos e normas relacionadas, buscando orientação sempre que não estiver absolutamente seguro quanto à aquisição, uso e/ou descarte de informações.

CAPÍTULO III DAS RESPONSABILIDADES ESPECÍFICAS

Art. 4º Entende-se por colaborador toda e qualquer pessoa física, contratada no regime estatutário, CLT ou temporário, e os prestadores de serviços, contratados por intermédio de pessoa jurídica ou não, que exerça alguma atividade dentro ou fora do RPPS.



§ 1º Os colaboradores deverão:

- I - manter sigilo das informações do RPPS;
- II - zelar pelos ativos de informação do RPPS, sejam eles físicos (processos, documentos, etc) ou digitais (arquivos, sistemas, etc);
- III - seguir as diretrizes e recomendações dos Conselhos e Gestores do RPPS quanto ao uso, divulgação e descarte de dados e informações.

§ 2º Será de inteira responsabilidade de cada colaborador, todo prejuízo ou dano que vier a sofrer ou causar ao RPPS e/ou a terceiros, em decorrência da não obediência às diretrizes e normas aqui referidas.

CAPÍTULO IV DO MONITORAMENTO E DA AUDITORIA DO AMBIENTE

Art. 5º Para garantir as regras mencionadas nesta PSI, o PREVIRESTINGA poderá:

- I - implantar sistemas de monitoramento nas estações de trabalho, servidores, correio eletrônico, conexões com a internet, dispositivos móveis ou wireless e outros componentes da rede – a informação gerada por esses sistemas poderá ser usada para identificar usuários e respectivos acessos efetuados, bem como material manipulado;
- II - tornar públicas as informações obtidas pelos sistemas de monitoramento e auditoria, no caso de exigência judicial ou solicitação do superior hierárquico;
- III - realizar, a qualquer tempo, inspeção física nos equipamentos em uso;
- IV - instalar sistemas de proteção, preventivos e detectáveis, para garantir a segurança das informações e dos perímetros de acesso.

CAPÍTULO V DO CORREIO ELETRÔNICO

Art. 6º O uso do correio eletrônico, seja através de email, seja através de mensagem eletrônica, é para fins corporativos e relacionados às atividades do colaborador usuário do RPPS, sendo terminantemente proibido:

- I - enviar mensagens não solicitadas para múltiplos destinatários, exceto se relacionadas a uso legítimo do PREVIRESTINGA;
- II - enviar mensagem por correio eletrônico usando o nome de usuário de outra pessoa ou endereço de correio eletrônico que não esteja autorizado a utilizar;
- III - enviar qualquer mensagem por meios eletrônicos que torne seu remetente e/ou o RPPS vulneráveis a ações civis ou criminais;
- IV - divulgar informações não autorizadas ou imagens de tela, sistemas, documentos e afinssem autorização expressa e formal concedida pelo proprietário desse ativo de informação;
- V - falsificar informações de endereçamento, adulterar cabeçalhos para esconder a identidade de remetentes e/ou destinatários, com o objetivo de evitar as punições previstas;
- VI - apagar mensagens pertinentes de correio eletrônico quando o RPPS estiver sujeito a algum tipo de investigação.



CAPÍTULO VI DA INTERNET

Art. 7º Exige-se dos colaboradores comportamento ético e profissional com o uso da internet utilizada pelo PREVIRESTINGA.

Art. 8º Os equipamentos, tecnologia e serviços utilizados para o acesso à internet são de responsabilidade do PREVIRESTINGA, que pode analisar e, se necessário, bloquear qualquer arquivo, site, correio eletrônico, domínio ou aplicação armazenados na rede/internet, estejam eles em disco local, na estação ou em áreas privadas da rede, visando assegurar o cumprimento de sua Política de Segurança da Informação.

§ 1º Qualquer informação acessada, transmitida, recebida ou produzida na internet está sujeita a divulgação e auditoria, tendo o RPPS, em total conformidade legal, o direito de monitorar e registrar todos os acessos a ela.

§ 2º Qualquer alteração dos parâmetros de segurança, por qualquer colaborador, sem o devido credenciamento e a autorização para tal, será julgada inadequada e os riscos relacionados serão informados ao colaborador e ao respectivo superior hierárquico.

§ 3º O uso de qualquer recurso para atividades ilícitas poderá acarretar as ações administrativas e as penalidades decorrentes de processos civil e criminal, sendo que nesses casos o PREVIRESTINGA cooperará ativamente com as autoridades competentes.

Art. 9º Somente os colaboradores que estão devidamente autorizados a falar em nome do RPPS para os meios de comunicação poderão manifestar-se, seja por e-mail, entrevista on-line, podcast, seja por documento físico, entre outros.

Art. 10. Apenas os colaboradores autorizados pelo PREVIRESTINGA poderão copiar, captar, imprimir ou enviar imagens da tela para terceiros, devendo atender à Lei Geral de Proteção de Dados, à Lei de Direitos Autorais, à proteção da imagem garantida pela Constituição Federal e demais dispositivos legais.

Art. 11. Os colaboradores com acesso à internet poderão fazer o download (baixa) somente de programas ligados diretamente às suas atividades no RPPS e deverão providenciar o que for necessário para regularizar a licença e o registro desses programas, desde que autorizados pelo Conselho Deliberativo.

§ 1º O uso, a instalação, a cópia ou a distribuição não autorizada de softwares que tenham direitos autorais, marca registrada ou patente na internet são expressamente proibidos.

§ 2º Os colaboradores não poderão em hipótese alguma utilizar os recursos do RPPS para fazer o download ou distribuição de software ou dados pirateados, atividade considerada delituosa de acordo com a legislação nacional.

Art. 12. É proibido o acesso, exposição, armazenamento, distribuição, edição, impressão ou gravação por meio de qualquer recurso, de materiais de cunho sexual.



Art. 13. Os colaboradores não poderão utilizar os recursos do RPPS para deliberadamente propagar qualquer tipo de vírus, worm, cavalo de troia, spam, assédio, perturbação ou programas de controle de outros computadores.

Art. 14. As regras expostas neste capítulo se aplicam no uso de computadores e outros dispositivos de uso do RPPS, bem como a dispositivos particulares dos usuários que estiverem conectados à internet (cabeadas ou sem fio).

CAPÍTULO VII DOS COMPUTADORES E OUTROS DISPOSITIVOS

Art. 15. Os computadores disponibilizados pelo PREVIRESTINGA aos colaboradores, constituem instrumento de trabalho para execução das atividades do RPPS.

§ 1º Cada colaborador deve zelar para segurança e bom uso dos equipamentos, reportando à área competente qualquer incidente que tenha conhecimento.

§ 2º Em caso de uso em desacordo com as instruções desta norma, o colaborador poderá ser responsabilizado.

CAPÍTULO VIII DA IDENTIFICAÇÃO E CONTROLE DE ACESSO

Art. 16. Para o acesso aos recursos tecnológicos do PREVIRESTINGA será exigido, sempre que possível, identificação e senha exclusiva de cada colaborador, permitindo assim o controle de acesso.

§ 1º É proibido o compartilhamento de login entre os colaboradores.

§ 2º Recomenda-se como boa prática de segurança que, ao realizar o primeiro acesso ao ambiente de rede local, o usuário seja direcionado a trocar imediatamente a sua senha.

§ 3º É de responsabilidade de cada usuário a memorização de sua própria senha, bem como a proteção e a guarda dos dispositivos de identificação que lhe forem designados.

§ 4º Os usuários podem alterar a própria senha, e devem ser orientados a fazê-lo, caso suspeitem que terceiros obtiveram acesso indevido ao seu login/senha.

CAPÍTULO IX DOS PROCEDIMENTOS DE CONTINGÊNCIA

Art. 17. Para garantir a segurança da informação, deverão ser realizadas cópias de segurança dos sistemas e respectivos bancos de dados utilizados pelo PREVIRESTINGA.

§ 1º As rotinas de cópia de segurança deverão, sempre que possível, ser realizadas de forma automatizada, em horários pré-definidos, devendo ainda ser realizadas verificações periódicas da sua execução e integridade.



§ 2º O armazenamento das cópias de segurança deverá ser planejado de forma que impeça o acesso a pessoas não autorizadas.

CAPÍTULO X DAS DISPOSIÇÕES FINAIS

Art. 18. Havendo descumprimento da presente Política de Segurança da Informação, aplicar-se-ão as penalidades previstas no Estatuto dos Servidores Municipais de Restinga Seca – RS, Lei Complementar Municipal nº 1/2007.

Art. 19. Os casos omissos deverão ser dirimidos pelo Conselho Deliberativo.

Restinga Sêca, 18 de dezembro de 2023.