

PREVCAR

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO – PSI

EDIÇÃO
2025



REGIME PRÓPRIO DE PREVIDÊNCIA SOCIAL DO MUNICÍPIO DE CARIRIAÇU - PREVCAR

PORTARIA Nº 2204001/2025

DISPÕE SOBRE A POLÍTICA DE SEGURANÇA DAS
INFORMAÇÕES - PSI E SUAS APLICAÇÕES NO REGIME
PRÓPRIO DE PREVIDÊNCIA SOCIAL (RPPS) DO
MUNICÍPIO DE CARIRIAÇU – PREVCAR.

O Diretor-Presidente do **Regime Próprio de Previdência Social de Caririaçu - PREVCAR**, Deusemar Pereira Vanderlei, nos exatos termos das atribuições previstas na Lei, no exercício das atribuições legais que lhe foram conferidas, torna pública a presente Portaria, para os fins legais e em atenção ao interesse público e à boa administração deste Fundo.

CONSIDERANDO que a informação é um ativo essencial da organização e precisa ser protegida quanto a eventuais ameaças, preservando e minimizando os riscos para a continuidade dos serviços prestados pelo RPPS;

CONSIDERANDO que a adoção de procedimentos que garantam a segurança das informações deve ser prioridade constante do RPPS, reduzindo os riscos de falhas, danos e prejuízos que possam comprometer os objetivos da instituição;

CONSIDERANDO que a política de segurança deve iniciar com o fortalecimento da cultura de proteção a informações;

CONSIDERANDO que o PREVCAR armazena informações cadastrais, funcionais e financeiras dos servidores segurados do RPPS do Município de Caririaçu e seus dependentes, bem como de seus próprios funcionários;

RESOLVE por meio da presente **PORTARIA**, prover e dar conhecimento a todos os servidores do PREVCAR, as regras que constituem as normas da **Política de Segurança da Informação - PSI**.



CAPÍTULO I FUNDAMENTOS DA PSI

Art. 1º- Um Programa de Segurança da Informação baseia-se em três princípios básicos:

I - Confidencialidade; Integridade; Disponibilidade.

- a) Confidencialidade: É a garantia de que a informação é acessível somente por pessoas autorizadas a terem acesso;
- b) Integridade: É a garantia da exatidão e inalterabilidade da informação e dos métodos de processamento;
- c) Disponibilidade: A disponibilidade é a garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

Art. 2º- Para os fins desta Política, considera-se:

- I - Ameaça: causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou uma organização;
- II - Ativo: qualquer coisa que tenha valor para a organização;
- III - Informação: agrupamento de dados que contenham algum significado;
- IV - Risco: combinação da probabilidade de um evento e de suas consequências;
- V - Vulnerabilidade: fragilidade de um ativo ou grupo de ativos que pode ser explorado por uma ou mais ameaças.

Art. 3º- As informações serão classificadas por níveis:

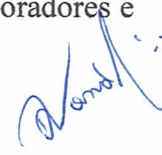
- I - Público: quando não há necessidade de sigilo;
- II - Interno: quando o acesso externo é restrito;
- III - Confidencialidade: quando o acesso é limitado a um usuário ou a um setor específico.

Parágrafo único - Os incisos II e III do caput deste artigo não se aplicam aos Órgãos de Controle.

CAPÍTULO II OBJETIVOS DA PSI

Art. 4º- 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. Estando lastreadas pelas diretrizes da Lei de nº 13.709, de 14 de Agosto de 2018 (LGPD – Lei Geral de Proteção de Dados) e suas alterações posteriores. 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. 5º- 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; e
- 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; e
 - c) Disponibilidade: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

CAPÍTULO III APLICAÇÕES DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Art. 6º- 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.

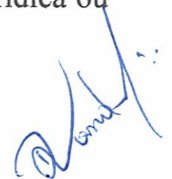
Parágrafo único - É obrigação de cada colaborador se manter atualizado em relação a esta PSI e aos procedimentos e normas relacionadas, buscando orientação sempre que não estiver absolutamente seguro quanto à aquisição, uso e/ou descarte de informações.

CAPÍTULO IV DAS RESPONSABILIDADES ESPECÍFICAS

Art. 7º- 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); e
- III - Seguir as diretrizes e recomendações da Diretoria Executiva 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 V DO MONITORAMENTO DE DA AUDITORIA DO AMBIENTE

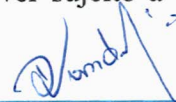
Art. 8º- Para garantir as regras mencionadas nesta PSI, o PREVCAR poderá:

- 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 de sua propriedade; e
- IV - Instalar sistemas de proteção, preventivos e detectáveis, para garantir a segurança das informações e dos perímetros de acesso.

CAPÍTULO VI DO USO DO CORREIO ELETRÔNICO

Art. 9º- O uso do correio eletrônico do RPPS é para fins corporativos e relacionados às atividades do colaborador usuário do PREVCAR, sendo terminantemente proibido:

- I - Enviar mensagens não solicitadas para múltiplos destinatários, exceto se relacionadas a uso legítimo do PREVCAR;
- II - Enviar mensagens 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 afins sem 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; e
- VI - Apagar mensagens pertinentes de correio eletrônico quando o RPPS estiver sujeito a algum tipo de investigação.



CAPÍTULO VII DO USO DA INTERNET

Art. 10. Exige-se dos colaboradores comportamento ético e profissional com o uso da internet disponibilizada pelo PREVCAR.

Art. 11. Os equipamentos, tecnologia e serviços fornecidos para o acesso à internet são de propriedade do PREVCAR, 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.

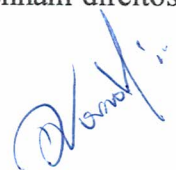
§3º- O uso de qualquer recurso para atividades ilícitas poderá acarretar em ações administrativas e em penalidades decorrentes de processos civil e criminal, sendo que nesses casos o PREVCAR cooperará ativamente com as autoridades competentes.

Art. 12. 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 online, podcast, seja por documento físico, entre outros.

Art. 13. Apenas os colaboradores autorizados pelo PREVCAR poderão copiar, captar, imprimir ou enviar imagens da tela para terceiros, devendo atender à norma interna de uso de imagens, à Lei de Direitos Autorais, à proteção da imagem garantida pela Constituição Federal e demais dispositivos legais.

Art. 14. Os colaboradores com acesso à internet poderão fazer o download (baixar) 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 pela Diretoria.

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

Art. 16. 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. 17. As regras expostas neste capítulo se aplicam no uso de computadores e outros dispositivos de propriedade do RPPS, bem como a dispositivos particulares dos usuários que estiverem conectados à internet do RPPS (cabeada ou sem fio).

CAPÍTULO VIII DO USO DE COMPUTADORES E OUTROS DISPOSITIVOS

Art. 18. Os computadores disponibilizados pelo PREVCAR aos colaboradores, constituem instrumento de trabalho para execução das atividades de negócio 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 mau uso, ou uso em desacordo com as instruções desta norma, o colaborador poderá ser responsabilizado.

CAPÍTULO IX IDENTIFICAÇÃO E CONTROLE DE ACESSO

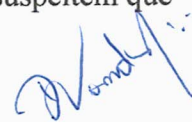
Art. 19. Para o acesso aos recursos tecnológicos do PREVCAR será exigido, sempre que possível, identificação e senha exclusiva de cada colaborador, permitindo assim o controle de acesso.

§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 X DO CUMPRIMENTO DAS ORIENTAÇÕES

Art. 20. O não cumprimento da Política de Segurança da Informação implica em falta grave e poderá resultar nas seguintes ações:

- a) advertência formal;
- b) suspensão;
- c) exoneração do cargo.

§ 1º- Respeitar-se-á o Estatuto dos Servidores Públicos de Caririaçu-CE no que se refere ao Regime Disciplinar ou outra Lei específica que a determine.

§ 2º- No que couber, outra ação disciplinar e/ou processo civil ou criminal poderá ser aplicado, a depender da gravidade da conduta.

CAPÍTULO XI PROCEDIMENTOS DE CONTINGÊNCIA

Art. 21. Para garantir a segurança da informação, deverão ser realizadas cópias de segurança dos sistemas e respectivos bancos de dados utilizados pelo PREVCAR.

§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.

Publique-se, registre-se e archive-se.

Caririaçu, 22 de abril de 2025.



DEUSEMAR PEREIRA VANDERLEI
Diretor-Presidente do PREVCAR
Portaria nº 128/2022