ESTADO DE PERNAMBUCO
MUNICIPIO DE CABO DE SANTO AGOSTINHO

INSTITUTO DE PREVIDÊNCIA SOCIAL DOS SERVIDORES DO MUNICÍPIO DO CABO DE SANTO AGOSTINHO - CABOPREV
PORTARIA Nº 009, DE 04 DE NOVEMBRO DE 2020

EMENTA: *Dispõe sobre a Política de Segurança da Informação – PSI, do Instituto de Previdência Social do Município do Cabo de Santo Agostinho-CABOPREV.*

O Diretor-Presidente do Instituto de Previdência Social dos Servidores Município do Cabo de Santo Agostinho – CABOPREV, JOSÉ ALBÉRICO SILVA RODRIGUES, Diretor-Presidente do CABOPREV, no uso de suas atribuições legais, tendo em vista o disposto no inciso III e V, do artigo 16, da Lei nº 3.342 de 22 de dezembro de 2017.

CONSIDERANDO a Lei nº 9.983, de 14 de julho de 2000: Altera o Decreto Lei nº 2848/40 – Código Penal, sobre tipificação de crimes por computador contra a Previdência Social e a Administração Pública.

CONSIDERANDO Lei nº 8.159, de 08 de janeiro de 1991, dispõe sobre a política nacional de arquivos públicos e privados e dá outras providências e alterações legais.

CONSIDERANDO a Lei de Acesso à Informação – Lei nº 12.527, de 18 de novembro de 2011, Decreto nº 7.724, de 16 de maio de 2012 e Decreto nº 7.845, de 14 de novembro de 2012.

CONSIIDERANDO o Marco Civil da Internet – Lei nº 12.965, de 23 de abril de 2014 e Decreto nº 8.771, de 11 de maio de 2016.

CONSIDERANDO a necessidade da criação de uma Política de Segurança da Informação para o Instituto, visando estabelecer diretrizes e padrões para garantir um ambiente tecnológico controlado e seguro de forma a oferecer todas as informações necessárias aos processos do CABOPREV, com integralidade, confidencialidade e disponibilidade.

CONSIDERANDO que o CABOPREV produz e recebe informações no exercício de suas competências constitucionais, legais e regulamentares, e que tais informações devem permanecer íntegras e disponíveis, bem como seu eventual sigilo deve ser resguardado.

CONSIDERANDO que a Política de Segurança da Informação – PSI é aspecto essencial para a adequada gestão da informação,

RESOLVE:

Art. 1º Instituir a Política de Segurança da Informação – PSI, do Instituto de Previdência Social dos Servidores do Município do Cabo de Santo Agostinho - CABOPREV, constituída por um conjunto de conceitos, objetivos, princípios, diretrizes, competências, responsabilidade e vedações, penalidades, revisão, disciplinados nos termos desta Portaria.

§1º Esta PSI aplica-se tanto ao ambiente informatizado quanto aos meios convencionais de processamento, comunicação e armazenamento da informação, bem como aos ambientes

físicos pertencentes ao patrimônio ou sob custódia, ambientes computacionais e ativos de informação pertencentes ou custodiados pelo CABOPREV.

§2º Todas as regras aqui estabelecidas deverão ser seguidas pelos servidores, diretores, conselheiros, estagiários, prestadores de serviços e demais contratados que executem atividade direta ou indiretamente ao CABOPREV, bem como, convênios, acordos, termos e outros instrumentos congêneres celebrados pelo Instituto.

CAPÍTULO I

DAS DISPOSIÇÕES PRELIMINARES E OBJETIVOS

Art. 2º A Política de Segurança da Informação – PSI, do CABOPREV, deve buscar preservar as informações e seus respectivos ativos quanto à confidencialidade, integridade, disponibilidade e autenticidade, tendo como objetivos:

I – contribuir para o cumprimento da missão do CABOPREV e a melhoria contínua dos resultados institucionais em prol dos segurados e da sociedade;

II – prover mecanismos de transparência e gestão das informações;

III – estabelecer diretrizes para a disponibilização e utilização de recursos de informação, serviços de redes de dados, estações de trabalho, internet, telecomunicações e correio eletrônico institucional;

IV – designar, definir ou alterar papéis e responsabilidades do grupo responsável pela PSI;
V – assegurar que fragilidades e incidentes em segurança da informação – SI sejam identificados para permitir a toma de ação corretiva e tempo hábil;

VI – possibilitar a criação de controles e promover a otimização dos recursos e investimentos em tecnologia da informação – TI, contribuindo com a minimização dos riscos associados;

VII – identificar os riscos que possam comprometer a confidencialidade, a integridade, a disponibilidade ou a autenticidade da informação, priorizando seu tratamento com base em critérios para aceitação de riscos compatíveis com os objetivos institucionais; e

VII – garantir que quaisquer usuários que tenham acesso por vinculo estatutário, funcional, contratual ou processual com o CABOPREV, entendam suas responsabilidades e atuem em consonância com os preceitos desta PSI, para que o risco de furto, fraude ou mau uso de informações não ocorra, ou seja, no mínimo, reduzido.

Art. 3º Para os fins desta Portaria aplicam-se as seguintes definições:

I – ativo de informações: qualquer informação que tenha valor para o CABOPREV; e

II – informação: conjunto de dados, textos, imagens, métodos, sistemas ou quaisquer formas de representação dotadas de significado em determinado contexto, podendo ser classificadas por:

pública: informação institucional ou de seus segurados com linguagem e formato dedicado à divulgação ao público em geral, podendo ocorrer devido ao cumprimento de legislação

vigente que exija publicidade, sendo seu caráter informativo ou promocional, sem a necessidade de sigilo;

interna: informação institucional sem o propósito de divulgação em que o acesso por parte de indivíduos externos à instituição deve ser evitado. Caso esta informação seja acessada indevidamente poderá causar danos a instituição e a seus segurados; e

restrita: é toda informação que pode ser acessada somente por usuários da instituição explicitamente indicado pelo nome ou por área que pertence. A divulgação não autorizada dessa informação pode causar sérios danos ao CABOPREV.
III – segurança da informação: proteção da informação contra ameaças a sua confidencialidade, integridade, disponibilidade e autenticidade para minimizar riscos, garantir a eficácia das ações do negócio e preservar a imagem do CABOPREV;

IV - confidencialidade: garantia de que a informação seja acessada somente pelas pessoas ou processos autorizados;

V - integridade: garantia de que a informação seja mantida em seu estado original, com o intuito de protegê-las, na guarda ou transmissão, contra alterações, gravações ou exclusões indevidas, intencionais ou acidentais;

VI – disponibilidade: garantia de que as informações estejam acessíveis às pessoas e aos processos autorizados, no momento requerido;

VII - autenticidade: propriedade que assegura a correspondência entre o autor de determinada informação e a pessoa, processo ou sistema a quem se atribui a autoria;

VIII – riscos: condições que criam ou aumentam o potencial de danos e perdas;

IX – cadastro: procedimento de criação de usuário para acesso à internet e/ou ter direito a utilização de e-mail institucional;

X – senha: conjunto alfanumérico de caracteres destinado a assegurar a identidade do usuário e a permitir seus acesso aos dados, programas e sistemas não disponíveis ao público, de uso pessoal e intransferível;

XI – colaborador: são usuários da informação, sendo o prestador de serviço terceirizado, consultor ou qualquer pessoa com vínculo transitório com o CABOPREV que tenha acesso, de forma autorizada, às informações ou as dependências do CABOPREV, bem como servidores do quadro de pessoal do CABOPREV, estagiários, Presidência, seus conselheiros e membros do Comitê de Investimentos.

XII – usuário da informação: servidor com vinculo institucional, interno ou externo, que tenha acesso, de forma autorizada, às informações ou às dependências do CABOPREV;

XIII – incidente de Segurança da Informação: qualquer indício de fraude, sabotagem, espionagem, desvio, falha ou evento indesejado ou inesperado que tenha probabilidade de comprometer ou ameaçar a SI; e

XIV – gestor da informação: Diretoria Executiva, bem como servidor responsável pela TI do CABOPREV.

CAPÍTULO II

DOS PRINCÍPIOS

Art. 4º São princípios básicos desta Política:

I – A preservação da imagem do Instituto e seus colaboradores, pois toda informação produzida ou recebida pelos colaboradores como resultado da atividade profissional pertence ao CABOPREV. As exceções devem ser explícitas e formalizadas.

II – Os equipamentos de informática e comunicação, sistemas e informações são utilizados pelos colaboradores para a realização das atividades profissionais. Excepcionalmente, o uso pessoal dos recursos é permitido desde que não prejudique o desempenho dos sistemas e serviços.

III - Deverá constar em contratos de prestação de serviços, celebrados com o CABOPREV, no que couber, Cláusula de Confidencialidade, como condição imprescindível para que possa ser concedido o acesso aos ativos de informação disponibilizados pelo Instituto.

IV - A responsabilidade em relação à segurança da informação deve ser comunicada na fase de contratação dos colaboradores. Todos os colaboradores devem ser orientados sobre os procedimentos de segurança, bem como o uso correto dos ativos, a fim de reduzir possíveis riscos. Eles devem assinar um termo de responsabilidade e de conhecimento desta Política, bem como de suas atualizações.

V – Que a segurança da informação esteja efetivamente incorporada, desde a concepção e por todo o ciclo de vida, em todos os processos executados pelo CABOPREV.

CAPÍTULO III

DAS DIRETRIZES DA PSI

Art. 5º As regras desta PSI, aqui estabelecidas, assim como aquelas constantes na legislação vigente são de observância obrigatória por todos os usuários do CABOPREV. Sua observância é de extrema importância para o adequado monitoramento do ambiente de TI, evitando a inadequada exposição de dados e a vulnerabilidade do sistema, a infestação dos programas com códigos maliciosos, utilização de softwares desatualizados, bem como eventuais instalações de softwares suspeitos, tendo como **diretrizes gerais**:

I – todos os colaboradores e aqueles que, de alguma forma, executem atividades vinculadas ao CABOPREV são corresponsáveis pela proteção e salvaguarda dos ativos e informações de que sejam usuários e dos ambientes a que tenham acesso, independente das medidas de segurança implementadas pelos responsáveis da gestão de segurança.

II - somente atividades lícitas, éticas e administrativamente admitidas devem ser realizadas, pelos usuários quando na utilização dos recursos de processamento da informação do CABOPREV.

III - a identificação do usuário por meio de senha é pessoal e intransferível, qualificando-o como responsável por todas as atividades desenvolvidas através dela.

IV – o cumprimento da Política de Segurança, pelos usuários, poderá ser auditado pelo CABOPREV.

V – o CABOPREV se reserva o direito de monitorar, automaticamente, o tráfego efetuado através das suas redes de comunicação, incluindo o acesso à Internet e o uso do Correio Eletrônico.

VI - os usuários deverão proteger o acesso a seus computadores através de tela de bloqueio a ser liberada mediante senha, quando os mesmos não estiverem em uso.

VII - além das cópias de segurança “backup” normalmente realizadas no servidor, será feita cópia de segurança adicional mantida em dispositivo externo com as informações codificadas (encriptografadas) em ambiente seguro para armazenagem fora do CABOPREV.

VIII - o acesso à internet é feito com tecnologia fornecida por operadora especializada.

IX - as informações em formato físico devem ser acondicionadas em armários específicos ou destruídas em triturador de papel, quando se tratar de documentos confidenciais a serem inutilizados.

X - esta Política define as Diretrizes para a Segurança da Informação, visando preservar a integridade, confidencialidade e disponibilidade das informações sob gestão do CABOPREV. Descreve a conduta considerada adequada para o manuseio, controle e proteção das informações contra destruição, modificação, divulgação indevida e acessos não autorizados, sejam acidentalmente ou intencionalmente, em consonância com o Código de Ética do Instituto.

Art. 6º Compreende as diretrizes quanto às **informações confidenciais**:

I – As informações produzidas e custodiadas devem ser classificadas de maneira a permitir o tratamento diferenciado, considerando o grau de importância, a criticidade, a sensibilidade e os requisitos legais, utilizando critérios definidos e observando o interesse público na informação.

II - São consideradas informações confidenciais, para os fins desta Política, quaisquer informações das partes consideradas não disponíveis ao público ou reservadas.
III - Informações confidenciais, quando impressas, deverão ser retiradas imediatamente das impressoras.

IV - Informações confidenciais impressas, quando não estiverem sendo utilizadas, deverão ser armazenadas em local fechado e seguro.

V - Nenhuma das informações confidenciais podem ser repassadas para terceiros sem consentimento por escrito do Diretor-Presidente do CABOPREV.

Art. 7º Compreende as diretrizes para **utilização da rede corporativa**:

I - O usuário é responsável pela própria e devida autenticação nos sistemas disponibilizados pelo CABOPREV, não podendo fornecer e/ou compartilhar seu usuário, senha e/ou acesso à rede com outros usuários.

II - O usuário está comprometido a utilizar as redes públicas e ou privadas do CABOPREV para uso exclusivo de atividades relacionadas ao setor no qual o usuário pertence.

III - É vedado o acesso a redes que disponibilizem conteúdos obscenos, pornográficos, eróticos, racistas, nazistas e de qualquer outro conteúdo que viole a lei, não podendo, ainda, ser exposto, armazenado, distribuído, editado ou gravado em quaisquer recursos tecnológicos do CABOPREV, nem na rede corporativa.

IV - O usuário deve garantir que as senhas de acesso à rede não sejam enviadas a outras pessoas, pois a senha é de uso pessoal, intransferível e sigilosa.

V – É de responsabilidade do usuário, autorizado pela Diretoria correspondente, o envio das informações a serem arquivadas no servidor institucional com o objetivo de manter o backup atualizado.

VI – Arquivos pessoais e/ou não pertinentes às atividades institucionais do CABOPREV (fotos, músicas, vídeos, etc.) não deverão ser copiados ou movidos para os drives de rede, pois podem sobrecarregar o armazenamento no servidor. Caso identificados, os arquivos poderão ser excluídos definitivamente sem necessidade de comunicação prévia do usuário.

VII – A internet deve ser utilizada para fins corporativos, enriquecimento intelectual ou como ferramenta de busca de informações, tudo que possa vir a contribuir para o desenvolvimento de atividades relacionadas ao CABOPREV.

VIII – Os acessos à internet serão monitorados, por meio de identificação e autenticação do usuário.

IX – É vedado a utilização do e-mail institucional para assuntos pessoais.
X – O correio eletrônico é uma ferramenta disponível e obrigatória para todos os usuários do CABOPREV, quando no exercício da atividade funcional ou em nome do CABOPREV.

XI – O usuário não poderá executar ou abrir arquivos anexados, enviados por remetentes desconhecidos ou suspeitos, com extensões do tipo: .bat, .exe, .Ink e .com, ou de quaisquer outros formatos alertados pela TI.

Art. 8º Compreende as diretrizes para **instalação e remoção de softwares**:

I - O usuário é proibido de instalar todo e qualquer programa não autorizado no computador e qualquer outro dispositivo computacional pertencente ao CABOPREV, salvo as instalações de programas que corroborem para o desempenho das atividades profissionais.

II - Caso o usuário necessite instalar ou remover qualquer software, deverá entrar em contato com o setor responsável.

III - É expressamente proibida a divulgação e/ou o compartilhamento indevido de informações sigilosas na internet.

IV - Os usuários poderão fazer download de arquivos da Internet que sejam necessários ao desempenho de suas atividades desde que observado os termos de licença de uso e registro desses programas.

V - O usuário deve utilizar a Internet de forma adequada e diligente.

VI - O usuário deve utilizar a Internet observando a conformidade com a lei, a moral, os bons costumes aceitos e a ordem pública.

VII - O usuário deve se abster de utilizar a Internet com objetivos ou meio para a prática de atos ilícitos, proibidos pela lei ou pela presente Política, lesivos aos direitos e interesses do Instituto ou de terceiros, ou que, de qualquer forma, possam danificar, inutilizar, sobrecarregar ou deteriorar os recursos

tecnológicos (hardware e software), bem como os documentos e arquivos de qualquer tipo, de seu uso ou de uso de terceiros.

VIII - O usuário é pessoalmente responsável por todas as atividades realizadas por intermédio de sua chave de acesso.

Art. 9º Compreende as diretrizes para **utilização de dispositivos móveis**:

I - É expressamente proibida a divulgação e/ou o compartilhamento indevido de informações sigilosas através de dispositivos móveis.

II - O usuário deve utilizar os dispositivos móveis de forma adequada e diligente, de forma a prevenir ações que possam danificar, inutilizar, sobrecarregar ou deteriorar os recursos tecnológicos (hardware e software), bem como os documentos e arquivos de qualquer tipo, de seu uso ou de uso de terceiros.

III - O usuário é pessoalmente responsável por todas as atividades realizadas por intermédio de dispositivos móveis, tanto por sua guarda quanto pelos conteúdos nele instalados.

Art. 10º Compreende as diretrizes para **utilização de acesso remoto à rede do CABOPREV**:

I - O usuário somente pode realizar acesso interativo entre redes onde a permissão esteja autorizada. A autorização depende das atividades profissionais relacionadas a função exercida.

Art. 11º Compreende as diretrizes para **utilização de contas e senhas de acesso**:

I – Todo usuário deve ter uma identificação única, pessoal e intrasferível, qualificando-o como responsável por qualquer atividade desenvolvida sob esta identificação que será responsável pelo sigilo da sua senha pessoal.

II – O usuário não deve armazenar as senhas anotadas em papel ou em arquivos, seja no computador ou em dispositivos móveis, de forma desprotegida ou seja, sem utilizar um meio de proteção, como, por exemplo, criptografia.

III - O usuário está proibido de utilizar contas e senhas de acesso pertencentes a outros usuários.

IV- Qualquer utilização, por meio da identificação e da senha de acesso, é de responsabilidade do usuário aos quais as informações estão vinculadas.

Art. 12º Compreende as diretrizes para **contratações e aquisições de serviços:**

I – Os acordos, convênios, ajustes e instrumentos congêneres sempre que possível, deverão dispor de especificações de segurança da informação que definam, no mínimo, SOS direitos de propriedade das informações, a classificação de sigilo, estabeleçam as regras para transferência de informações e os acordos de confidencialidade e não divulgação. Devem, ainda, prever a concordância com os procedimentos de segurança pelos seus empregados, prepostos ou representantes, sem prejuízo da participação em orientações complementares de segurança da informação que o CABOPREV julgar necessário.

II – As contratações de tecnologia devem ser precedidas de análise de risco e da classificação de segurança das informações, nos termos da legislação pertinente em vigor.

III – As contratações que envolvam a utilização de computação em nuvem devem conter cláusulas que estabeleçam a territorialidade de dados, garantam interoperabilidade, transferência e migração dos dados após seu encerramento.

Art. 13º Compreende as diretrizes para Controle de Acesso Físico:

I - Devem ser adotados controles que restrinjam a entrada e saída de visitantes, pessoal interno, equipamentos, mídias e documentos físicos, estabelecendo perímetros de segurança e habilitando o acesso apenas de pessoal autorizado.

II - O ambiente físico em que se encontram os equipamentos servidores e equipamentos de rede é de acesso exclusivo aos integrantes do TI e a outros, excepcionalmente, mediante autorização do Chefe do TI e devidamente acompanhados por técnico.

CAPÍTULO IV

DAS COMPETÊNCIAS E RESPONSABILIDADES

Art. 14º A Diretoria Executiva, no âmbito do cumprimento desta Portaria, tem por competência:

I – Formular e conduzir diretrizes para a PSI, bem como analisar periodicamente sua efetividade;

II – Cumprir e fazer cumprir esta PSI;

III – realizar ações necessárias para implementação e monitoramento de práticas de Segurança da Informação -SI;

IV – revisar normas e procedimentos inerentes à SI;

V – apoiar a Tecnologia da Informação – TI, na definição de processos de trabalho e de procedimentos operacionais necessários à proteção de suas informações;

VI – conscientizar os usuários e quaisquer servidores sob sua supervisão em relação aos conceitos e às práticas de SI;

VII – incorporar aos processos de trabalho de sua Diretoria, práticas inerentes à SI; e

VIII – tomar as medidas administrativas necessárias para que sejam adotadas ações corretivas em tempo hábil em casos de comprometimento da SI do CABOPREV.

Art. 15º Compete aos usuários da informação:

I – cumprir fielmente com esta PSI;

II – buscar orientação da TI do CABOPREV, em caso de dúvidas relacionadas à SI;

III – proteger as informações contra acesso, modificação, destruição ou divulgação não-autorizadas;

IV – assegurar que os recursos tecnológicos à sua disposição sejam utilizados apenas para as finalidades relacionadas ao CABOPREV;

V – cumprir as leis e as normas que regulamentam os aspectos de propriedade intelectual;

VI – comunicar, imediatamente, à Comissão de Ética do CABOPREV, quando do descumprimento ou violação desta PSI;

VII – utilizar de forma ética, legal e consciente os recursos computacionais e informacionais do CABOPREV;

VIII – garantir a SI sob sua posse, conforme os critérios definidos pelo respectivo gestor da informação;

IX – comunicar, tempestivamente, ao gestor da informação sobre situações que comprometam a SI sob custódia; e

X – comunicar aos gestor da informação eventuais limitações para o cumprimento dos critérios por ele definido com vistas à proteção da informação.

Art. 16º Compete à TI do CABOPREV, no que concerne às informações sob sua guarda:

I – zelar pela eficácia dos controles de Sistema de Informação utilizados e informar ao Diretor –Presidente os riscos residuais;

II – planejar, implantar, fornecer e monitorar a capacidade de armazenagem, processamento e transmissão necessários para garantir a segurança requerida pelas áreas internas do CABOPREV;

III – atribuir conta ou dispositivo de acesso a computadores, sistemas, base de dados e qualquer outro ativo de informação a um responsável identificável como pessoa física, responsável pelo uso da conta;

IV - monitorar as estações de trabalho, servidores, correio eletrônico, conexões com a internet, dispositivos móveis ou wireless e outros componentes da rede, de modo que a informação gerada por esses sistemas possa ser usada para identificar usuários e respectivos acessos efetuados, bem como material manipulado;

V – solicitar mensalmente relatório de logs de acesso junto ao Departamento de Tecnologia da Informação do CABOPREV;

VI – definir as regras para instalação de software e hardware em ambiente de produção corporativo, bem como em ambiente educacional e/ou dedicados à visitação externa, exigindo o seu cumprimento dentro do CABOPREV;

VII – propor ajustes, melhorias, aprimoramentos e modificações desta PSI;

VIII – convoca e coordenar reuniões que discutam a respeito desta PSI; e

IX – prover todas as informações de gestão de SI do CABOPREV.

Parágrafo único. No caso de identificação do descumprimento das normas vedadas nesta PSI, o responsável pela DTI do CABOPREV, deverá comunicar ao Diretor-Presidente para, a qualquer tempo, revogar credenciais de acesso concedidas a usuários em virtude do descumprimento desta PSI ou das normas e procedimentos específicos dela decorrentes.

CAPÍTULO V

DAS VEDAÇÕES E PENALIDADES

Art. 17º O cumprimento das regras estabelecidas por esta PSI é obrigatório e, sua não observância, além de afetar diretamente o CABOPREV, acarretará penalidades ao seu infrator.

Art. 18º São consideradas violações, além daquelas previstas na legislação própria, as seguintes condutas:

I – uso ilegal de software;

II – introdução (intencional ou não) de malwares;

III – tentativas de acesso não autorizados a dados e sistemas;

IV – compartilhamento de informações sigilosas institucionais ou de segurados;

V – instalação de software sem a devida homologação;

VI – atualização de software sem o devido acompanhamento; e

VII – acesso a sites com conteúdo pornográficos, ilegais ou obscenos.

Parágrafo único. É considerado malwares arquivos como: worm, vírus, trojan, ransomware, keylogger, etc, pela rede do CABOPREV, de modo que o "click" em links desconhecidos, suspeitos ou sem o devido parâmetro de segurança são propícios à atividade maliciosa.

Art. 19º São proibidas as seguintes atividades com relação ao uso de e-mails:

I – envio de informações privadas do CABOPREV, sem autorização da Diretoria;

II – envio de e-mail usando o nome de outro usuário;

III – envio de spam;

IV – falsificação de executáveis maliciosos;

V – envio de executáveis maliciosos;

VI – envio de conteúdo pornográfico, ilegal ou obsceno;

VII – envio de mensagem com o caráter ofensivo, desrespeitoso, degradante, infame, ameaçador entre outros; e

VIII – envio de softwares pirateados, sem a devida licença.

Art. 20º É proibida a execução de programas que tenham como finalidade a decodificação de senhas, o monitoramento da rede, a leitura de dados de terceiros, a propagação de vírus de computador, a destruição parcial ou total de arquivos ou a indisponibilidade de serviços.

Art. 21º É terminantemente proibido o uso de softwares ilegais (sem licenciamento) nos computadores do CABOPREV.

Parágrafo único. A TI do CABOPREV poderá valer-se deste instrumento para desinstalar, sem aviso prévio, todo e qualquer software sem licença de uso, em atendimento à Lei Federal nº 9.609, de 19 de fevereiro de 1998. "que dispõe sobre a proteção da propriedade intelectual de programa de computador, sua comercialização no País".

Art. 22º Toda tentativa de alteração dos parâmetros de segurança, por qualquer usuário, sem o devido credenciamento e a autorização para tal, será considerada inadequada e os riscos relacionados serão informados ao usuário e ao respectivo Diretor correspondente.

Art. 23º O não cumprimento das disposições constantes nesta Política de Segurança da Informação e Comunicações, suas

normas e procedimentos agregados caracteriza infração, a ser apurada, sujeitando o infrator às penalidades previstas no Código de Ética e na Lei nº 1.554/90 que institui o Regime Jurídico Único para os Servidores Públicos do Município do Cabo de Santo Agostinho, regulamentada pela Lei nº 6.123/1968 do Estatuto dos Funcionários Públicos Civis do Estado de Pernambuco.

Art. 24º A apuração das infrações será realizada pela Comissão de Ética do CABOPREV estabelecida no Código de Ética, como também propor a abertura de processo administrativo disciplinar, após análise dos fatos e autorização do Diretor-Presidente.

CAPÍTULO VI

DA REVISÃO DA PSI

Art. 25º A Política de Segurança da Informação e Comunicações deve ser revisada sempre que necessário ou em um intervalo não superior a 03 (três) anos.

CAPÍTULO VII

DAS DISPOSIÇÕES FINAIS

Art. 26º A presente PSI deve ser observada e respeitada como parte fundamental da cultura interna do CABOPREV e, por tal razão, qualquer incidente que caracterize infringência às suas normas será ato contra as normas e políticas do CABOPREV.

Parágrafo único. O não cumprimento dos requisitos previstos nesta PSI, das normas complementares e nos procedimentos de SI, acarretará violação às regras internas do CABOPREV e sujeitará o usuário às medidas administrativas e legais cabíveis.

Art. 27º Para a uniformização da informação organizacional, esta PSI deverá ser comunicada a todos servidores do CABOPREV a fim de que seja cumprida dentro e fora da Autarquia.

Art. 28º Arquivos e geral, mesmo aqueles deletados, ocupam espaço em disco, por essa razão deverão ser evitadas a criação de cópias desnecessárias ou pessoais em ambiente de trabalho, uma vez que podem comprometer o desempenho do computador, resultando, portanto, em inadequado desempenho do serviço.

Art. 29º Dispositivos móveis ou mídias digitais devem ser conectados com cautela aos computadores, uma vez que podem conter arquivos com as mais variadas espécies de vírus.

Art. 30º Os casos omissos, as situações especiais e demais diretrizes necessárias à implantação desta Política devem ser analisados pelo setor responsável pela segurança da informação no CABOPREV.

Art. 31º Os usuários deverão tomar conhecimento formal desta Política, além de ser concedido treinamento para facilitar o entendimento e a comunicação.

Art. 32º Todos os usuários que se utilizarem de Informações e Sistemas de Informação, no âmbito do CABOPREV, devem assinar o Termo de Uso dos Sistemas de Informações e Termo de Responsabilidade e Sigilo da Informação, constante do Anexo I.

§1º A assinatura dos Termos previstos no caput deste artigo se darão durante o processo de admissão, nomeação ou posse, momento em que será apresentada a PSI do CABOPREV.

Havendo um número expressivo de pessoal, o TI poderá realizar esta atividade, bem como a palestra de divulgação e sensibilização da PSI do CABOPREV, de forma centralizada, em local e data oportuna;

§2º No caso de Comissionados, Celetistas e Efetivos, deverão assinar os Termos previstos no caput deste artigo em prazo a ser definido pelo TI;

§3º No caso de prestadores de serviço, a assinatura dos Termos previstos no caput deste artigo se darão durante atividade de divulgação e sensibilização da PSI do CABOPREV, antes de ser concedido a eles acesso as informações e sistemas de informação;

§4º Após a assinatura dos Termos, o usuário assume formalmente a responsabilidade pelo bom uso dos ativos de informações, o compromisso de seguir a PSI-CABOPREV e de manter o sigilo, no prazo legal, sobre todos os ativos de informações e processos, mesmo após o seu desligamento ou término de prestação de serviços.

Art. 33º Deverão ser observados os princípios constantes do Código de Ética do Instituto.

Art. 34º Por ocasião do desligamento de qualquer empregado, o setor responsável pela segurança da informação deverá providenciar o imediato cancelamento de todas as senhas de acesso aos sistemas corporativos bem como do correio eletrônico.

Art. 35º Esta Portaria entra em vigor na data de sua publicação.

Cabo de Santo Agostinho, 04 de novembro de 2020

JOSÉ ALBÉRICO SILVA RODRIGUES
Diretor-Presidente do CABOPREV

ANEXO I

Termo de Responsabilidade e Sigilo da Informação

Eu, _____, RG nº _____, CPF nº _____,

Função/cargo/Prestador de Serviços: _____,

Sob a matrícula funcional/Contrato nº ___,

Nos termos da Política de Segurança da Informação do Instituto de Previdência Social dos Servidores do Município do Cabo de Santo Agostinho-CABOPREV, declaro que tenho pleno conhecimento de minhas responsabilidades no que concerne ao sigilo que deve ser mantido em relação aos ativos e informações sigilosas das quais tenha tido acesso ou possa vir a acessar ou ter conhecimento, em decorrência das atividades funcionais desempenhadas no exercício do cargo, função ou prestação de serviço no âmbito do CABOPREV, ou fora do mesmo.

Comprometo-me a guardar o sigilo necessário a que sou obrigado, estando ciente das penalidades nos termos da legislação vigente, especialmente dos art. 153 e art. 325 do Código Penal (Decreto-lei n. º 2.848, de 07 de dezembro de 1940) e demais legislações constantes do verso, bem como de quaisquer sanções administrativas que poderão advir.

A vigência da obrigação de sigilo, assumida pela minha pessoa por meio deste termo, terá validade enquanto a informação não for tornada de conhecimento público por qualquer outra pessoa

ou entidade, ou mediante autorização escrita, concedida à minha pessoa pelas partes interessadas neste termo.

Neste Termo, as seguintes expressões serão assim definidas:

Informação Sigilosa significará toda informação, apresentada sob forma escrita, verbal ou por quaisquer outros meios, que possui restrição de acesso público em razão de sua criticidade para a segurança da sociedade, do município e do Instituto.

Informação Sigilosa inclui, mas não se limita à informação relativa às operações, processos, planos ou intenções, informações sobre produção, instalações, equipamentos, sistemas, dados, habilidades especializadas, projetos, métodos e metodologia, fluxogramas, especializações, componentes, fórmulas, produtos e questões relativas ao desempenho das atividades laborais.

Cabo de Santo Agostinho, _____, de _____ de _____.

_____
(Assinatura do Usuário)
Servidor (Contratado)

VERSO
COMPROMISSO LEGAL
CÓDIGO PENAL BRASILEIRO

DIVULGAÇÃO DE SEGREDO – Art. 153 § 1º. A divulgar, sem justa causa, informações sigilosas ou reservadas, assim definidas em Lei, contidas ou não nos sistemas de informações ou banco de dados da Administração Pública: Pena – detenção de 1(um) a 4(quatro) anos e multa.
INVASÃO DE DISPOSITIVO INFORMÁTICO – Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita: Pena – detenção, de 3 (três) meses a 1 (um) ano, e multa (Lei 12.737/2012).

INSERÇÃO DE DADOS FALSOS EM SISTEMA DE INFORMAÇÕES – Art. 313-A Inserir ou facilitar, o funcionário autorizado, a inserção de dados falsos, alterar ou excluir indevidamente dados corretos nos sistemas informatizados ou banco de dados da Administração Pública com o fim de obter vantagem indevida para si ou para outrem ou para causar dano: Pena – reclusão de 2(dois) a 12(doze) anos e multa.

MODIFICAÇÃO OU ALTERAÇÃO NÃO AUTORIZADA DE SISTEMA DE INFORMAÇÕES – Art. 313-B. Modificar ou alterar, o funcionário, sistema de informação ou programa de informática sem autorização ou solicitação de autoridade competente: Pena – detenção de 3(três) meses a 2(dois) anos e multa. Parágrafo único: As penas são aumentadas de um terço até a metade se a modificação ou alteração resulta em dano para a Administração Pública ou para o administrado.

FALSIDADE IDEOLÓGICA – Art. 299 – Omitir, em documento público ou particular, declaração que dele deva constituir, ou nele inserir, fazer inserir declaração falsa ou diversa da que deva ser escrita, com fim de prejudicar direito, criar obrigação ou alterar a verdade sobre fato juridicamente relevante. Pena – Reclusão de 01 (um) a 05 (cinco) anos e multa se o documento é público, e reclusão de 01 (um) a 03 (três) anos e multa se o documento é particular. Parágrafo único – Se o agente é funcionário público e comete o crime prevalecendo-se do cargo ou se a falsificação ou alteração é de

assentamento de registro civil, aumenta-se a pena da sexta parte.
VIOLAÇÃO DE SIGILO FUNCIONAL – Art. 325 – Revelar fato de que tem ciência em razão do cargo e que deva permanecer em segredo, ou facilitar-lhe a revelação: Pena: detenção, de seis meses a dois anos, ou multa, se o fato não constitui crime mais grave.
Art. 325 § 1º-Nas mesmas penas deste artigo incorre quem: I – permite ou facilita, mediante atribuição, fornecimento e empréstimo de senha ou qualquer outra forma, o acesso de pessoas não autorizadas a sistema de informações ou banco de dados da Administração Pública, II – se utiliza, indevidamente, do acesso restrito. § 2º - Se da ação ou omissão resulta dano à Administração Pública ou a outrem: Pena – reclusão, de 2 (dois) a 6 (seis) anos, e multa.

FUNCIONÁRIO PÚBLICO – Art. 327 – Considera-se funcionário público para os efeitos penais, quem, embora transitoriamente ou sem remuneração, exerce cargo, emprego ou função pública. Art. 327 § 1º – Equipara-se a funcionário público quem exerce cargo, emprego ou função em entidade paraestatal e quem trabalha para empresa prestadora de serviço contratada ou conveniada para execução de atividade típica da Administração Pública. Art. 327 § 2º – A pena será aumentada da terça parte quando os autores dos crimes previstos neste capítulo, forem ocupantes de cargos em comissão ou de função de direção ou assessoramento de órgão da administração direta, sociedade de economia mista, empresa pública ou fundação instituída pelo poder público.

Termo de Uso dos Sistemas de Informação

Eu, _____, RG nº _____, CPF nº _____,

Função/cargo/Prestador de Serviços: _____,

Sob a matrícula funcional/Contrato nº _____,

CONSIDERANDO que o CABOPREV:

a) disponibiliza a infraestrutura tecnológica, como ferramenta de trabalho, para o pleno desenvolvimento das atividades profissionais;
b) detém a exclusiva propriedade da infraestrutura tecnológica disponibilizada;
c) torna explícito que não há expectativa de privacidade sobre os ativos, informações e recursos institucionais, tendo em vista que os mesmos são destinados para fins profissionais;
d) pode haver prejuízos pela má utilização dos recursos disponibilizados;

DECLARO, estar ciente e ter pleno conhecimento:

a) da Política de Segurança da Informação do Instituto de Previdência Social dos Servidores do Cabo de Santo Agostinho - CABOPREV, apresentada na entrevista de admissão e disponibilizada de inteiro teor na Intranet;
b) da realização do monitoramento dos recursos tecnológicos disponibilizados, indispensável para a manutenção do nível de segurança adequado da organização;
c) de que o CABOPREV pode realizar auditoria interna sobre os recursos de hardware e software disponibilizados para as atividades profissionais e;
d) que o descumprimento da PSI-CABOPREV está sujeito às sanções previstas na Lei nº 1.554/90 que institui o Regime Jurídico Único para os Servidores Públicos do Município do Cabo de Santo Agostinho, regulamentada pela Lei nº 6.123/1968 do Estatuto dos Funcionários Públicos Civis do Estado de Pernambuco, cláusulas contratuais e demais legislações vigentes, sem prejuízo das ações penal, civil e

administrativa, previstas em legislação específica, respeitados os princípios constitucionais do contraditório e da ampla defesa.

Cabo de Santo Agostinho, _____, de ___ de _____.

_____
(Assinatura)

Publicado por:
Maria Amélia Lemos do Monte Câmara
Código Identificador:7296D128

Matéria publicada no Diário Oficial dos Municípios do Estado de Pernambuco no dia 06/11/2020. Edição 2703
A verificação de autenticidade da matéria pode ser feita informando o código identificador no site:
http://www.diariomunicipal.com.br/amupe/