

Portaria N° /2022, de de julho de 2022

EMENTA: Dispõe sobre diretrizes e orientações de procedimentos de Política de Segurança da Informação e Comunicações, que visam conscientizar e orientar os servidores do Instituto de Previdência dos Servidores Públicos do Município do Jaboatão dos Guararapes – JABOATÃOOPREV.

LUCILEIDE FERREIRA LOPES, Presidente do Instituto de Previdência dos Servidores Públicos do Município do Jaboatão dos Guararapes, no uso de suas atribuições que lhe confere o Inciso VI do Art. 54º da Lei nº 108/2001,

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.

CONSIDERANDO 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 e Comunicações para o Instituto.

RESOLVE:

Art. 1º - Publicar a Política de Segurança da Informação e Comunicações do JABOATÃOOPREV, conforme Anexo desta Resolução.

Art. 2º — Esta Resolução entrará em vigor na data de sua publicação.

ANEXO

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO DO INSTITUTO DE PREVIDÊNCIA DOS SERVIDORES PÚBLICOS DO MUNICÍPIO DO JABOATÃO DOS GUARARAPES — JABOATÃOPREV.

1. JUSTIFICATIVA

Para cumprimento da missão do JABOATÃOPREV é de vital importância que a informação seja protegida, cuidada e gerenciada adequadamente com o objetivo de garantir sua disponibilidade, integridade, confidencialidade, legalidade e auditabilidade, independentemente do meio de armazenamento, processamento ou transmissão que esteja sendo utilizado.

O desenvolvimento e a implantação da Política de Segurança da Informação e Comunicações é uma importante ferramenta para combater ameaças ao Instituto. Esta Política é um conjunto de diretrizes e orientações de procedimentos que visam conscientizar e orientar os servidores do quadro de pessoal do JABOATÃOPREV, estagiários, Presidência, seus conselheiros e membros do Comitê de Investimentos, cujo objetivo primeiro é definir o tratamento que deve ser dado às informações armazenadas, processadas ou transmitidas no ambiente convencional ou no ambiente tecnológico, visando a credibilidade do Regime Próprio de Previdência Social do Município do Jaboatão dos Guararapes, gerido pelo JABOATÃOPREV, perante seus segurados e a sociedade.

Para fins de apuração do comprometimento com a Política de Segurança da Informação e Comunicações, entende-se por servidor público todo aquele que, por força de lei, contrato ou de qualquer ato jurídico, preste serviços de natureza permanente, temporária ou excepcional, ainda que sem retribuição financeira, desde que ligado direta ou indiretamente a qualquer órgão do poder estatal, como as autarquias, as fundações públicas, as entidades paraestatais, as empresas públicas e as sociedades de economia mista, ou em qualquer setor onde prevaleça o interesse do Estado.

2. OBJETIVOS

A Política de Segurança da Informação e Comunicações do JABOATÃOPREV tem como objetivos:

I - Estabelecer diretrizes estratégicas que orientem e apoiem as ações institucionais em segurança, com o intuito de preservar, em qualquer meio:

- a) Confidencialidade: propriedade que garante que a informação seja acessada somente pelas pessoas ou processos que tenham autorização para tal;

- b) Integridade: propriedade que garante a não violação das informações com intuito de protegê-las contra alteração, gravação ou exclusão indevida, acidental ou proposital;
- c) Disponibilidade: propriedade que garante que as informações estejam acessíveis às pessoas e aos processos autorizados, no momento requerido;
- d) Autenticidade: propriedade que assegura a correspondência entre o autor de determinada informação e a pessoa, processo ou sistema a quem se atribui a autoria;

As orientações aqui apresentadas são os princípios fundamentais e representam como o JABOATÃOOPREV exige que a informação seja utilizada.

II — Promover práticas de segurança da informação, compatíveis com o uso aceitável das informações e dos ativos que as suportam, de forma a minimizar riscos e criar um ambiente seguro para a realização das atividades do Instituto.

3. ABRANGÊNCIA

A Política de Segurança da Informação e Comunicações do JABOATÃOOPREV aplica-se a:

- a) Todos os ambientes físicos pertencentes ao patrimônio ou sob a custódia do JABOATÃOOPREV;
- b) Todos os ambientes computacionais e ativos de informação pertencentes ou custodiados pelo JABOATÃOOPREV;
- c) Todos os contratos, convênios, acordos, termos e outros instrumentos congêneres celebrados pelo JABOATÃOOPREV;
- d) Todos os Servidores, Estagiários, Prestadores de Serviço, Presidência, seus conselheiros e membros do Comitê de Investimentos.

Esta Política também se aplica, no que couber, ao relacionamento do JABOATÃOOPREV com outros órgãos e entidades públicos ou privados.

4. PRINCÍPIOS

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 JABOATÃOOPREV. 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 JABOATÃOPREV, 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 JABOATÃOPREV.

5. DIRETRIZES

5.1 DIRETRIZES GERAIS

I — Todos os colaboradores e aqueles que, de alguma forma, executem atividades vinculadas ao JABOATÃOPREV 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 JABOATÃOPREV.

III — O cumprimento da Política de Segurança, pelos usuários, poderá ser auditado pelo JABOATÃOPREV.

IV — O JABOATÃOPREV 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 Corporativo.

V - 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.

VI – Será feita cópia de segurança “backup” periodicamente dentro do servidor do JABOATÃOOPREV.

VII - O acesso à internet é feito com tecnologia fornecida por operadora especializada.

VIII - As informações em formato físico devem ser acondicionadas em armários específicos ou destruídas, quando se tratar de documentos confidenciais a serem inutilizados.

IX - Esta Política define as Diretrizes para a Segurança da Informação, visando preservar a integridade, confidencialidade e disponibilidade das informações sob gestão do JABOATÃOOPREV. 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.

5.2 DIRETRIZES PARA 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 da Presidente do JABOATÃOOPREV.

5.3 DIRETRIZES PARA UTILIZAÇÃO DA REDE

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

II - É proibido o acesso a redes que disponibilizem conteúdos obscenos, pornográficos, eróticos, racistas, nazistas e de qualquer outro conteúdo que viole a lei.

III - 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.

5.4 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 JABOATÃO PREV, 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.

5.5 DIRETRIZES PARA UTILIZAÇÃO DA INTERNET

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

II - 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.

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

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

V - 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.

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

5.6 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.

5.7 DIRETRIZES PARA UTILIZAÇÃO DE ACESSO REMOTO À REDE DO JABOATÃO PREV

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.

5.8 DIRETRIZES PARA UTILIZAÇÃO DE CONTAS E SENHAS DE ACESSO

I - 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.

II - As senhas de acesso tem caráter pessoal, e é intransferível, cabendo ao seu titular total responsabilidade quanto ao seu sigilo.

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

5.9 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 JABOATÃO PREV 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.

5.10 DIRETRIZES PARA CÓPIA DE SEGURANÇA

I – Deverá ser realizada com periodicidade a cópia de segurança “Backup” dos arquivos digitais armazenados na rede compartilhada dos servidores.

II – A cópia consistirá em armazenamento de dados em “Nuvem” com acesso limitado.

III – Todos os arquivos das unidades que compõem o órgão JaboaãoPrev deverão ter uma cópia de segurança armazenado em sistema seguro.

6. PENALIDADES

I — 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 na Resolução 001/2020 do JABOATÃOPREV que institui o Código de Ética e na Lei nº 224/1996 que Institui o Estatuto do Servidor Público Municipal do Município de Jaboatão dos Guararapes.

II- A apuração das infrações será realizada pela Comissão de Ética estabelecida no Código de Ética, como também propor a abertura de processo administrativo disciplinar, após análise dos fatos e autorização da Presidente.

7. ATUALIZAÇÕES

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

8. DISPOSIÇÕES FINAIS

I — Os casos omissos, as situações especiais e demais diretrizes necessárias à implantação desta Política devem ser analisados pela Diretoria Executiva do JABOATÃOPREV.

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

III - Deverão ser observados os princípios constantes do Código de Ética do Instituto.

IV - Por ocasião do desligamento de qualquer empregado, deverá se providenciar o imediato cancelamento de todas as senhas de acesso aos sistemas corporativos bem como do correio eletrônico.

GLOSSÁRIO

ATIVO	Meios de armazenamentos, transmissão e processamento, sistemas de informação, bem como os locais onde se encontrem esses meios e as pessoas que a eles têm acesso.
COLABORADORES	Servidores do quadro de pessoal do JABOATÃOPREV, estagiários, Presidência, seus conselheiros e membros do Comitê de Investimentos.
USUÁRIOS	Para efeito desta Política, denominados como Colaboradores.