POLÍTICA COMPLEMENTAR DE SEGURANÇA DA INFORMAÇÃO – PSI

Institui a Política Complementar de Segurança da Informação - PSI da SUBSECRETARIA DE GESTÃO PREVIDENCIÁRIA - SUPREV, e dá outras providências.

1. INTRODUÇÃO

A Política Complementar de Segurança da Informação, ou simplesmente "PSI" é um documento que orienta e estabelece as diretrizes corporativas da SUPREV para a proteção dos ativos de informação e prevenção de responsabilidade legal para todos os usuários. Deve, portanto, ser cumprida e aplicada em todas as áreas.

A presente Política Complementar de Segurança da Informação está baseada nas recomendações da norma ABNT NBR ISO/IEC 27005:2008, reconhecida mundialmente como um código de prática para a gestão da segurança da informação.

A informação é um ativo de grande valor para a SUPREV, por isso, necessita ser adequadamente protegida.

2. OBJETIVOS

Estabelecer diretrizes que permitam aos servidores, fornecedores e prestadores de serviços da SUPREV seguirem padrões de comportamento relacionados à segurança da informação adequados às necessidades operacionais e de proteção legal da instituição e do indivíduo.

Garantir que os recursos computacionais e serviços de Tecnologia da Informação - TI serão utilizados de maneira adequada. O usuário deve conhecer as regras para utilização da informação de maneira segura, evitando exposição que possa prejudicar a SUPREV, colaboradores e terceiros.

Nortear a definição de normas e procedimentos específicos de segurança da informação, bem como a implementação de controles e processos para seu atendimento. Deve implementar controles para preservar os interesses da SUPREV contra danos que possam ser consideradas como violação ao uso dos serviços e, portanto, considerados proibidos.

Preservar as informações da SUPREV quanto à:

- **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.

- **Confidencialidade:** garantia de que o acesso à informação seja obtido somente por pessoas autorizadas.

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

Caso os procedimentos ou normas aqui estabelecidos sejam violados por usuários, a SUPREV informará aos órgãos competentes de forma que sejam tomadas medidas cabíveis.

3. APLICAÇÕES

As diretrizes estabelecidas deverão ser seguidas por todos os servidores, bem como os fornecedores e prestadores de serviço que se aplicam à informação em qualquer meio ou suporte.

Esta política complementar dá ciência a cada servidor, fornecedor e prestador de serviços de que os ambientes, sistemas, computadores e redes poderão ser monitorados e gravados, conforme previsto nas leis brasileiras.

É também obrigação de cada servidor se manter atualizado em relação a esta política complementar e aos procedimentos e normas relacionadas, buscando orientação do seu gestor ou da área de tecnologia de informação sempre que não estiver absolutamente seguro quanto à aquisição, uso e/ou descarte de informações.

Toda informação produzida ou recebida pelos servidores como resultado da atividade profissional contratada pela SUPREV pertence à referida instituição.

As exceções devem ser explícitas e formalizadas em contrato entre as partes. Os equipamentos de informática e comunicação, sistemas e informações são utilizados pelos servidores para a realização das atividades profissionais. O uso pessoal dos recursos é permitido dentro dos limites cabíveis, desde que não prejudique o desempenho dos sistemas e serviços.

A SUPREV poderá registrar todo o uso dos sistemas e serviços, visando garantir a disponibilidade e a segurança das informações utilizadas.

4. DAS RESPONSABILIDADES ESPECÍFICAS

DOS SERVIDORES E FORNECEDORES EM GERAL

Entende-se por servidor toda e qualquer pessoa física, nomeada por concurso público que exerça alguma atividade dentro ou fora da instituição.

Entende-se por fornecedor o prestador de serviço por intermédio de pessoa jurídica ou não, que exerça alguma atividade dentro ou fora da instituição.

Será de inteira responsabilidade cada servidor ou fornecedor todo prejuízo ou dano que vier a sofrer ou causar da SUPREV e/ou a terceiros, em decorrência da não obediência às diretrizes e normas referidas.

DOS SERVIDORES EM REGIME DE EXCEÇÃO (TEMPORÁRIOS E ESTAGIÁRIOS):

Devem entender os riscos associados à sua condição especial e cumprir rigorosamente o que está previsto na Política Complementar de Segurança da Informação - PSI.

A concessão de acesso poderá ser revogada a qualquer tempo se for verificado que a justificativa de motivo de negócio não mais compensa o risco relacionado ao regime de exceção ou se o

colaborador que o recebeu não estiver cumprindo as condições definidas nesta política complementar.

DOS GESTORES DE PESSOAS E/OU PROCESSOS:

Ter postura exemplar em relação à segurança da informação, servindo como modelo de conduta para os servidores sob a sua gestão.

Atribuir aos servidores, na fase de contratação e de formalização dos contratos individuais de trabalho, de prestação de serviços ou de parceria, a responsabilidade do cumprimento da Política Complementar de Segurança da Informação.

Exigir dos servidores a assinatura do Termo de Compromisso e Ciência, assumindo o dever de seguir as normas estabelecidas, bem como se comprometendo a manter sigilo e confidencialidade, mesmo quando desligado, sobre todos os ativos de informações da SUPREV.

Adaptar as normas, os processos, procedimentos e sistemas sob sua responsabilidade para atender a esta política complementar.

DA EQUIPE DE TECNOLOGIA DA INFORMAÇÃO:

Toda estrutura de equipe segue Instrução Normativa nº 37/2020, itens 4.4 e 5.2.

5. DO MONITORAMENTO E DA AUDITORIA DO AMBIENTE

Toda estrutura do monitoramento e da auditoria do ambiente seguem o Decreto nº15.423, de 19 de dezembro de 2013, Art. 1° e § 1º, e a Instrução Normativa nº 037/2020, itens 4.7, 4.8 e 5.1.

CONTROLE DO USO DE E-MAIL:

As diretrizes a serem seguidas quanto ao controle do uso de e-mail seguem o Decreto nº15.423, de 19 de dezembro de 2013 e Instrução Normativa nº 10/2015.

CONTROLE DO USO DE INTERNET:

As normas de controle do uso de Internet encontram-se descritas na Instrução Normativa nº 08/2014.

CONTROLE DE ACESSO À INFORMAÇÃO SENSÍVEL DE MEIO FÍSICO:

O objetivo é prevenir o acesso não autorizado às informações sensíveis de meio físico de posse e competência da SUPREV, evitando danos e interferências.

O acesso à área em que são processadas e armazenadas as informações sensíveis de meio físico são controlados e restrito às pessoas autorizadas. O acesso não autorizado não será permitido.

O controle de retirada e/ ou consulta das informações será controlado por responsável designado que fará monitoramento por meio de emissão de protocolos. As informações contidas no protocolo contam com no mínimo:

- nome e visto do servidor responsável emissor do protocolo;
- nome e visto do servidor interessado ao acesso da informação sensível de meio físico;
- a data e hora da retirada e/ou consulta da informação sensível de meio físico;
- a data e hora da devolução da informação sensível de meio físico e
- Observações Complementares.

A retirada de informações sensíveis de meio físico sem a devida emissão do protocolo não será autorizada.

Toda a informação sensível de meio físico será conferida no ato da devolução, estando sujeito a emissão de ocorrências em caso de desorganização, desleixo ou ausência de documentos.

São considerados os casos de desorganização e desleixo:

- Desordem na numeração das folhas do processo;
- Rasuras, anotações e amassados;
- Sujeiras de alimentos e bebidas.

Não é permitido a retirada de qualquer folha objeto de complemento ao arquivo de informação.

A possibilidade de foto cópia será permitida somente com a emissão do protocolo, onde deverá ser preenchido no item “Observações Complementares” as folhas que foram objeto da foto cópia.

Não é permitido a locomoção de informações sensíveis de meio físico fora as dependências da SUPREV.

6. IDENTIFICAÇÃO:

Os dispositivos de identificação e senhas protegem a identidade do servidor usuário, evitando e prevenindo que uma pessoa se faça passar por outra perante a SUPREV e/ou terceiros.

O uso dos dispositivos e/ou senhas de identificação de outra pessoa constitui crime tipificado no Código Penal Brasileiro (art. 307–falsa identidade). Tal norma visa estabelecer critérios de responsabilidade sobre o uso dos dispositivos de identificação e deverá ser aplicada a todos os servidores.

Todos os dispositivos de identificação utilizados na SUPREV, como o número de registro do colaborador, as identificações de acesso aos sistemas, os certificados e assinaturas digitais e os dados biométricos têm de estar associados a uma única pessoa física.

O usuário, vinculado a tais dispositivos identificadores, será responsável pelo seu uso correto perante a instituição e a legislação (cível e criminal). Todo e qualquer dispositivo de identificação pessoal, portanto, não poderá ser compartilhado com outras pessoas em nenhuma hipótese.

Se existir login de uso compartilhado por mais de um colaborador, a responsabilidade perante a SUPREV e a legislação (cível e criminal) será dos usuários que dele se utilizarem. Somente se for identificado conhecimento ou solicitação do gestor de uso compartilhado ele deverá ser responsabilizado.

É proibido o compartilhamento de login para funções de administração de sistemas.

A área de tecnologia de informação responde pela criação da identidade lógica dos servidores na instituição.

Devem ser distintamente identificados os visitantes, estagiários, empregados temporários, empregados regulares e prestadores de serviços, sejam eles pessoas físicas e/ou jurídicas. Ao realizar o primeiro acesso ao ambiente de rede local, o usuário deverá trocar imediatamente a sua senha conforme as orientações apresentadas.

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.

As senhas não devem ser anotadas ou armazenadas em arquivos eletrônicos (Word, Excel, etc.), compreensíveis por linguagem humana (não criptografados).

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.

Todos os acessos devem ser imediatamente bloqueados quando se tornarem desnecessários.

Caso o servidor necessite trocar sua senha, ele deverá utilizar o serviço automatizado de troca de senha através do portal trocasenha.pbh.gov.br ou realizar a solicitação no portal de atendimento da Prodabel (https://atendimentoprodabel.pbh.gov.br)

As normas de identificação e senhas para acesso ao Correio Eletrônico, encontram-se dispostas na Instrução Normativa nº 10/2015.

O descumprimento da Política de Segurança da Informação da Prefeitura de Belo Horizonte acarretará aplicações de sanções conforme disposto no Decreto nº 15.423, Art. 10.

7. COMPUTADORES E RECURSOS TECNOLÓGICOS

As normas do uso de computadores e recursos tecnológicos da SUPREV encontram-se dispostas na Instrução Normativa nº 37/2020, itens 4.3, 4.4, 4.5 e 4.6.

8. PRIVACIDADE DA INFORMAÇÃO

Define-se como necessária a proteção da privacidade das informações, aquelas que pertencem aos seus segurados e/ou beneficiários e que são manipuladas ou armazenadas nos meios às quais a SUPREV detém total controle administrativo, físico, lógico e legal.

As diretivas abaixo refletem os valores institucionais da SUPREV e reafirmam o seu compromisso com a melhoria contínua desse processo:

- As informações são coletadas de forma ética e legal, com o conhecimento do segurado / beneficiário, para propósitos específicos e devidamente informados;

- As informações são acessadas somente por pessoas autorizadas e capacitadas para seu uso adequado;

- As informações podem ser disponibilizadas a empresas contratadas para prestação de serviços, sendo exigido de tais organizações o cumprimento de nossa política complementar e diretivas de segurança e privacidade de dados;

- As informações e dados constantes de nossos cadastros, bem como outras solicitações que venham garantir direitos legais só são fornecidos aos próprios interessados, mediante solicitação formal, seguindo os requisitos legais vigentes.

9. DISPOSITIVOS MÓVEIS

As normas sobre a utilização de dispositivos móveis estão dispostas na Instrução Normativa nº 37/2020, item 4.3.7

10. DATACENTER

As diretrizes e procedimentos para serviço de hospedagem no Data Center encontram-se dispostas na Instrução Normativa nº 17/2017.

11. PROCEDIMENTOS DE BACKUP

As normas dos procedimentos de Backup encontram-se dispostas no Mapeamento, Modelagem e Documentação do Procedimento para Realização e Recuperação de Cópias de Segurança de Sistemas e Banco de Dados da Prodabel.

12. VIOLAÇÃO DA POLÍTICA, ADVERTÊNCIA E PUNIÇÕES

Ao detectar uma violação da política complementar, a primeira coisa a fazer é determinar a sua razão, ou seja, verificar se a violação ocorreu por negligência, acidente, erro ou por desconhecimento da política complementar vigente.

Nos termos da Política Complementar de Segurança da Informação e todas as Normas, Decretos e Instruções Normativas acimas desta, a Prodabel procederá ao bloqueio do acesso ou ao cancelamento do usuário, caso seja detectado uso indevido com o intuito de prejudicar o andamento do trabalho ou pôr em risco a imagem da instituição.

É recomendado o treinamento dos usuários em segurança da informação, por meio de cartilhas, com o intuito de divulgar e conscientizar os funcionários e demais colaboradores sobre a política complementar de segurança a ser seguida por todos. O programa de treinamento em segurança deve fazer parte do programa de integração de novos usuários. Os treinamentos de reciclagem devem ser previstos quando necessários.

Caso seja necessário advertir o usuário pelo não cumprimento das normas estabelecidas neste documento, devem ser informados o superior imediato e o departamento de Recursos Humanos para interagir e manterem-se informados da situação.

O funcionário colaborador poderá ser aplicado a penalidade no caso de irregularidade comprovada.

De acordo com a infração cometida, as seguintes punições serão: comunicação de descumprimento, advertência ou suspensão e demissão por justa causa.

Fica desde já estabelecido que não há progressividade como requisito para a configuração da dispensa por justa causa, podendo a Diretoria, no uso do poder diretivo e disciplinar que lhe é atribuído, aplicar a pena que entender devida quando tipificada a falta grave.

13. DAS DISPOSIÇÕES FINAIS

Assim como a ética, a segurança deve ser entendida como parte fundamental da cultura interna da SUPREV. Ou seja, qualquer incidente de segurança subentende-se como alguém agindo contra a ética e os bons costumes.

Sua elaboração e revisão deverão ser precedidos pela SUPREV, sendo posteriormente aprovado por órgão superior competente.

As normas aqui descritas deverão sofrer alterações sempre que necessário, sendo que estas deverão ser registradas pela SUPREV, aprovada por órgão superior competente e divulgadas pelo própria SUPREV, dentro da sua estrutura organizacional, considerando-se do o tempo hábil para eventuais providências sejam tomadas.

Os requisitos estabelecidos nesta Política Complementar de Segurança da Informação se fazem obrigatórios, devendo ser seguido por todos os servidores e prestadores de serviço que acessem informações da SUPREV.

Na ausência de qualquer determinação que não conste nesta Política Complementar, os servidores e prestadores de serviços, ficam sujeitos aos critérios estabelecidos na Política de Segurança da Informação da Prefeitura de Belo Horizonte, Decreto nº 15.423, de 19 de dezembro de 2013, e demais Políticas e/ou Instruções Normativas superiores.

14. TERMO DE CIÊNCIA E CONHECIMENTO

TERMO DE CIÊNCIA E CONHECIMENTO DA POLÍTICA COMPLEMENTAR DE SEGURANÇA DA INFORMAÇÃO - PSI DA SUPREV

Declaro que recebi a Política Complementar de Segurança da Informação - PSI da SUPREV, estando ciente de seu conteúdo e da sua importância para o bom exercício funcional da própria SUPREV.

A assinatura do presente Termo, anexo a referida Política Complementar de Segurança da Informação, é manifestação de minha concordância e do meu compromisso em cumpri-lo integralmente.

Belo Horizonte/MG, _____ de _____ de 20____.

_____
Nome Completo
Matrícula