ATA DA 55ª (QUINQUAGÉSIMA QUINTA) REUNIÃO EXTRAORDINÁRIA DO CONSELHO MUNICIPAL DE PREVIDÊNCIA DO CAMPREV

05/11/2020

Aos cinco dias do mês de novembro do ano de dois mil e vinte, às 14h00 na sala de reunião situada no aplicativo "Google Meet" realizou-se a quinquagésima quinta Reunião Extraordinária do Colegiado, sob a presidência do Sr. José Erivan Leite de Araújo, Presidente do CMP, a qual foi secretariada por mim, Denílson Pereira de Albuquerque, Secretário do CMP. **I - ABERTURA:** Havendo número legal de Conselheiros foi, pela Mesa, declarada aberta a reunião na qual estiveram presentes os Conselheiros: Aldaíria Calixto de Medeiros, Daniel Lange de Souza, Daniel Lovato, Denílson Pereira de Albuquerque, José Erivan Leite de Araújo, Irani Cândida dos Santos Montanhez, Kátia Maria Constâncio Caparroz, Marcelo Henrique de Paula, Maria Elvira Moreira Pavarini, Nivaldo Camilo de Campos, Sidney Vieira Costacurta e Tânia Maria Amorim de Oliveira. **II - PAUTA:** Análise/discussão e aprovação da Política da Segurança da Informação e análise final do Relatório de Gestão Atuarial da Instituição nos termos do documento apresentado pela Diretoria Executiva - SEI CAMPREV. 2019.00001752-89. **III - DOCUMENTO RECEBIDO - SEI:** 2020. 1752-89; Assunto: Política de Segurança da Informação. O Presidente deu início à reunião saudando os presentes e agradecendo a presença de todos. Em seguida, foi efetuada a leitura da pauta do dia supracitada, bem como do documento referente à Política de Segurança da Informação, objeto da pauta do dia. Após a leitura os Conselheiros analisaram detalhadamente ponto por ponto o documento e foram propostas, por vários Conselheiros, diversas alterações, com o intuito de aprimorar a Política de Segurança da Informação e dar maior segurança às informações, bem como melhorar a transparência. Essas alterações foram incorporadas ao documento enviado ao CMP pela Diretoria Executiva e esse documento será parte integrante desta Ata. **IV - DELIBERAÇÕES: 1 -** Foi aprovada por unanimidade a Política de Segurança da Informação, com as alterações propostas pelos Conselheiros e anotadas no expediente enviado pela Diretoria Executiva e que fica fazendo parte integrante desta Ata**. 2 -** Enviar ofício para a Diretoria Executiva com a deliberação pela aprovação da Política de Segurança da Informação, com as alterações propostas pelos Conselheiros. **3 -** Ficou convencionado que a

análise a respeito do Relatório de Gestão, em sua parte final, dar-se-á em reunião a ser marcada oportunamente. **V - ENCERRAMENTO**: Nada mais havendo a ser tratado, o Presidente agradeceu a presença dos conselheiros e deu por encerrada a reunião. Do que, para constar, foi lavrado a presente Ata sendo assinada por mim, Denílson Pereira de Albuquerque (_____) Secretário do CMP, que a lavrei, pelo presidente do CMP e demais conselheiros presentes, estando devidamente de acordo com os termos acima.

Política da Segurança da Informação

1. **Introdução**

1.1. Este documento descreve a Política da Segurança da Informação – PSI do Instituto de Previdência Social do Município de Campinas - CAMPREV detalhando as definições, objetivos, responsabilidades, diretrizes e vedações relativos ao tema.

2. **Das Definições**

2.1. Informação: é todo dado e conhecimento que tenha valor para uma organização ou indivíduo. É um ativo essencial para toda organização a fim de cumprir a sua missão e, portanto, deve ser adequadamente protegido;

2.2. Segurança da Informação: é a proteção da informação de vários tipos de ameaças, para garantir a continuidade do negócio da organização;

2.3. Os conceitos relacionados à Segurança da Informação são, entre outros:

a) Confidencialidade: propriedade que limita o acesso à informação tão somente às entidades legítimas, ou seja, àquelas autorizadas pelo proprietário da informação;

b) Integridade: propriedade que garante que a informação manipulada mantenha todas as características originais estabelecidas pelo proprietário da informação;

c) Disponibilidade: propriedade que garante que a informação esteja sempre disponível para o uso legítimo, ou seja, por aqueles usuários autorizados pelo proprietário da informação;

d) Autenticidade: propriedade que garante que a informação é proveniente da fonte anunciada e que não foi alvo de mutações ao longo de um processo.

2.4. Política de Segurança da Informação: fornece orientação e apoio dos gestores para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações

pertinentes;

2.5. Servidor de Arquivos: recurso computacional, que armazena os dados do Instituto necessários para sua operação, compartilhando as informações entre seus colaboradores através de acessos autorizados formalmente e onde são executados procedimentos de cópias de segurança.

3. **Dos Objetivos**

3.1. Definir através dessa PSI um conjunto de diretrizes que protejam as informações do Instituto e dos seus beneficiários, ao mesmo tempo em que promovam a transparência das informações de interesse público;

3.2. Obter o comprometimento e apoio de todos os níveis gerenciais;

3.3. Contribuir para a melhoria contínua dos processos operacionais do Instituto através do monitoramento e revisão constante da implantação da PSI.

4. **Das Responsabilidades**

4.1. Área de Tecnologia da Informação

a) Elaborar a PSI do Instituto de acordo com a cultura organizacional, as normas definidas pela Diretoria Executiva, assim como as boas práticas de segurança da informação e governança digital, contribuindo para as suas atualizações quando necessárias;

b) Notificar a Diretoria Executiva periodicamente sobre novos riscos identificados no ambiente ou que tenham surgido na tecnologia utilizada no momento;

c) Elaborar e manter Normas e Procedimentos alinhados com essa PSI. Planejar e promover a implementação, manutenção e atualização de toda a infraestrutura de Tecnologia de Informação - TI do Instituto;

d) Gerir os sistemas de proteção do Instituto e seus ativos, notificando a Diretoria Executiva a respeito de suas deficiências, fatores de riscos e possíveis soluções;

e) Implementar os controles necessários para vulnerabilidades potenciais e necessidades de proteção.

4.2. Diretoria Executiva

a) Revisar e aprovar a PSI e suas atualizações, de acordo com as necessidades específicas de cada área;

b) Promover e conscientizar a utilização da PSI, no âmbito do Instituto como um todo, assim como nas suas respectivas áreas de atuação;

c) Decidir pelas ações a serem tomadas quando de ocorrências de descumprimento da política de segurança.

4.3. Setor Jurídico

a) Orientar sobre legislações e suas mudanças que devam ser contempladas na PSI relativas à segurança da informação.

4.4. Setor de Recursos Humanos

a) Assegurar-se de que os servidores, estagiários e prestadores de serviços comprovem, por escrito, estar cientes do conteúdo da PSI;

b) Comunicar à Área de Tecnologia da Informação qualquer mudança no quadro de colaboradores que implique em alteração de acessos aos sistemas e ferramentas tecnológicas do Instituto.

4.5. Colaboradores do Instituto (Servidores, Estagiários e Prestadores de Serviço)

a) Seguir as orientações dessa PSI;

b) Cuidar das informações que estão sob sua guarda e responsabilidade, zelando continuamente pela proteção das informações do Instituto ou de seus beneficiários contra acesso, modificação, destruição ou divulgação não autorizada;

c) Garantir que os sistemas e informações sob sua responsabilidade estejadequadamente protegidos;

d) Cumprir as leis e normas que regulamentam os aspectos de propriedade intelectual;

e) Comunicar imediatamente à área de Tecnologia da Informação qualquer descumprimento da Política de Segurança da Informação;

f) Assegurar que os recursos (computacionais ou não) colocados à sua disposição sejam utilizados apenas para as finalidades do Instituto.

g) Reportar tempestivamente à área de Tecnologia da Informação os incidentes em segurança da informação de que tenham ciência ou suspeita.

h) Colaborar, em suas áreas de competência, na identificação e no tratamento de incidentes em segurança da informação.

5. **Das Diretrizes**

5.1. Diretrizes Gerais:

5.1.1. A PSI está alinhada com a estratégia geral do Instituto e deve ser periodicamente revisada para contemplar as necessidades e desafios específicos da organização;

5.1.2. A PSI deve ser divulgada para todos os colaboradores pelo gestor do respectivo setor, desde o momento em que iniciam suas atividades no Instituto, assim como deve ser reforçada continuamente através de treinamentos e orientações gerenciais;

5.1.3. O acesso ao e-mail corporativo deve ser disponibilizado a todos os servidores do instituto, e deverá ser utilizado para comunicação entre o público interno e externoAs dúvidas relativas a essa PSI sejam no seu conteúdo, assim como na sua aplicação prática, deverão ser feitas à área de Tecnologia da Informação para orientações;

5.1.4. Quaisquer mudanças na necessidade de acessos a e-mail, internet e sistemas de informações devem ser comunicadas oficialmente pela Chefia imediata do colaborador à Área de Tecnologia da Informação para os devidos ajustes nos respectivos acessos.

5.2. Utilização de Internet

5.2.1. O uso da internet deve ser de forma consciente, para que se mantenha o nível de qualidade de serviço oferecido a todos os colaboradores;

5.2.2. A utilização deve ser priorizada para as atividades operacionais do Instituto e que não o exponha a ameaças externas;

5.2.3. Acessos diferenciados do padrão, como acesso a redes sociais, utilização de armazenamento em nuvem e sítios de streaming de vídeos, devem ser justificados e solicitados à Área de Tecnologia da Informação em formulário específico, com aprovação da Chefia Imediata do colaborador.

5.3. Utilização de e-mail corporativo e pessoal

5.3.1. O acesso ao e-mail corporativo deve ser disponibilizado a todos os servidores do instituto, e deverá ser utilizado para comunicação entre o público interno e o externo.

5.3.2. O e-mail corporativo é de uso intransferível, através de senha que será regulada por informação detalhada em Normas e Procedimentos;

5.3.3. O e-mail pessoal é permitido desde que não exponha o Instituto e seja utilizado de maneira adequada.

5.4. Acesso aos Sistemas de Informação

5.4.1. As senhas utilizadas para acesso aos sistemas de informação, utilizados no Instituto, não devem ser compartilhadas entre os colaboradores;

5.4.2. O acesso aos sistemas de informação necessários às operações do Instituto deve ser solicitado à área de Tecnologia de Informação em formulário específico e aprovado pela Chefia imediata do colaborador.

5.5. Acesso e utilização dos dados em Servidor de Arquivos

5.5.1. Acesso às pastas compartilhadas no servidor de informações deve ser solicitado à Área de Tecnologia da Informação em formulário específico que deve ser aprovado pela Chefia Imediata;

5.5.2. Apenas arquivos relativos aos procedimentos operacionais do Instituto devem ser armazenados no Servidor de Arquivos;

5.5.3. Os dados do Instituto são sigilosos e não poderão ser expostos sem a devida autorização.

5.6. Armazenamento de dados

5.6.1. Os arquivos de uso pessoal do colaborador podem ser armazenados nos seus computadores locais, desde que não infrinjam quaisquer leis sobre direitos autorais, assim como não possibilitem o risco de segurança por uso de malware ou outros programas nocivos similares.

5.6.2. Os arquivos de uso do Instituto para suas rotinas operacionais devem ser armazenados no Servidor de Arquivos para permitir um adequado controle de acesso às informações e a realização de cópias de segurança.

5.7. Utilização de equipamentos de informática externos

5.7.1. Computadores externos somente poderão ser conectados à rede do Instituto após avaliação da Área de Tecnologia de Informação quanto à viabilidade do uso, assim quanto aos riscos apresentados, sendo preferencialmente de uso temporário.

5.8. Utilização de equipamentos de informática de propriedade do Instituto

5.8.1. A configuração física ou lógica de equipamentos de informática do Instituto, sejam eles estações de trabalho do tipo computadores “desktop” ou notebooks, impressoras ou scanners, deverá ser realizada somente pela Área de Tecnologia da Informação ou por prestadores de serviço contratados para este fim;

5.8.2. Somente aplicativos homologados pela Área de Tecnologia da Informação poderão ser instalados nos computadores do Instituto;

5.8.3. Os notebooks de propriedade do Instituto são de utilização temporária, assim como o armazenamento de informações dos mesmos. Quaisquer dados que precisem ser armazenados definitivamente devem ser transferidos para o Servidor de Arquivos, onde são realizados procedimentos de cópias de segurança.

5.8.4. A TI poderá valer-se deste instrumento para desinstalar, sem aviso prévio, todo e qualquer software sem licença de uso, em atendimento à Lei 9.609/98 (Lei do Software).

6. **Das vedações**

6.1. Propagação ou execução de qualquer tipo de malware, tais como worm, virus, trojan, ransomware, keylogger, etc., pela rede do Instituto;

6.2. Instalação e uso de programas ilegais no ambiente corporativo; 6.3.Armazenamentos de arquivos não relacionados às atividades operacionais do

Instituto no Servidor de Arquivos;

6.4. Utilização indevida de dados corporativos, divulgação não autorizada de informações, segredos comerciais ou outras informações sem a permissão expressa do Instituto;

6.5. Uso de dados, informações, equipamentos, software, sistemas ou outros recursos tecnológicos, para propósitos ilícitos, que possam incluir a violação de leis, de regulamentos internos e externos, da ética ou de exigências de organismos reguladores da área de atuação do Instituto.

6.6. A identificação do usuário (senha) é pessoal e intransferível, sendo vedada a utilização desta por outra pessoa. O colaborador que emprestou a senha deverá ser qualificado como responsável por todas as atividades desenvolvidas através dela.

6.7. Será vedada a entrada de pessoas não autorizadas ao Data Center. A entrada nesta área ou partes dedicadas às atividades específicas de TI, por pessoas não autorizadas (visitantes, prestadores de serviço, terceiros e até mesmo funcionários), que necessitarem ter acesso físico ao local, somente será permitida quando acompanhados de pessoas autorizadas.

7. **Das Sanções**

7.1. Nos casos em que houver violação desta política, sanções administrativas e/ou legais poderão ser adotadas.

7.2. O funcionário infrator poderá ser notificado e a ocorrência da transgressão imediatamente comunicada ao seu gestor imediato, à diretoria correspondente e à Presidência.

8. **Disposições finais**

8.1.Esta Política de Segurança entra em vigor na data da sua publicação.

José Erivan Leite de Araújo	**Denílson Pereira de Albuquerque**
Presidente CMP	**Secretário CMP**