POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

DO INSTITUTO DE PREVIDÊNCIA DOS SERVIDORES PÚBLICOS

DO MUNICÍPIO DE CURITIBANOS (PSI IPESMUC).

DISPOSIÇÕES PRELIMINARES

A política de segurança da informação do IPESMUC tem por objetivo estabelecer normas e procedimentos a serem seguidos por todos os servidores vinculados ao RPPS, visando a preservação da segurança das informações que por ali circulam e por eles são divulgadas. Com isso, o IPESMUC busca assegurar a continuidade dos serviços prestados com a redução dos riscos pelo vazamento de informações confidenciais.

FINALIDADE

I. Estabelecer diretrizes para o cumprimento de padrões de comportamento adequados, visando a segurança da informação, por parte dos colaboradores, fornecedores e demais pessoas que acessem às dependências do IPESMUC;
II. Definir normas e procedimentos específicos para a segurança da informação, além de controles internos visando o atendimento destas normas;
III. Fomentar o gerenciamento de riscos, além de prevenir e minimizar os impactos provenientes de possíveis incidentes ligados a segurança dos ativos não físicos do RPPS;
IV. Evitar o acesso aos sistemas e informações confidenciais por pessoas não autorizadas;
V. Preservar quesitos como: **integridade** (garantir que a informação seja mantida em seu estado original); **confidencialidade** (garantir que a informação seja acessada somente a quem for endereçada) e; **disponibilidade** (garantir que a informação esteja presente quando for solicitada).

ABRANGÊNCIA

O presente documento se aplica a todos os funcionários, fornecedores, prestadores de serviços e demais pessoas que acessem as dependências do instituto, bem como, os usuários que tiverem acesso a e-mails corporativos e sistemas, serão abarcados por este documento.

DADOS FUNCIONAIS

Os dados dos funcionários, sejam efetivos, temporários ou estagiários, estarão resguardados junto ao Departamento de Recursos Humanos da prefeitura de Curitibanos/SC. Esses dados não serão disponibilizados para terceiros, exceto por demanda judicial, além dos dados digitais (e-mails, acesso a sistemas diversos), que são de responsabilidade e custódia do setor de T.I..

CORREIO ELETRÔNICO

A utilização do correio eletrônico (e-mail corporativo) do instituto deve ser feita de maneira responsável, para fins corporativos, relacionados a assuntos e atividades desenvolvidas pelo funcionário do IPESMUC, sendo terminantemente proibido:

I. Enviar mensagens com *link's* para acesso a plataformas/sites que não tenham relação com o dia-a-dia e rotinas do trabalho no instituto;
II. Enviar mensagens utilizando um e-mail ou nome de usuário que não for o seu e/ou não esteja autorizado a utilizar;
III. Encaminhar mensagens que possam causar ao RPPS danos a sua reputação e que possam ensejar ações cíveis ou criminais;
IV. Apagar mensagens do e-mail e demais plataformas de comunicação do instituto, em qualquer hipótese;
V. Divulgar informações de captura de tela, sistemas e documentos, sem autorização do proprietário da informação.

INTERNET

Quanto ao uso de internet, os servidores do IPESMUC devem observar padrões de comportamento ético e profissional das ferramentas de busca e demais funções. Além disso, os equipamentos, serviços e *softwares* fornecidos são de propriedade do IPESMUC, podendo, se necessário, bloquear qualquer arquivo/*link* suspeito que esteja na rede e/ou na área privada do usuário.

Qualquer informação recebida, transmitida ou produzida está sujeita a monitoramento, e, em caso de utilização de qualquer desses recursos para prática de atividade delituosa, serão aplicadas as medidas administrativas correspondentes, além das penalidades correspondentes de processos cíveis ou criminais.

É inteiramente proibida a participação em salas de bate-papo (*Google Talk*, *Skype* etc.) exceto aqueles de exclusivo interesse para desenvolvimento das atividades do instituto.

PARÂMETRO DE SEGURANÇA

Os parâmetros de segurança, assim como os níveis de acesso à informação, são de responsabilidade da T.I., observando o cargo em questão e as responsabilidades inerentes a ele. Qualquer alteração nos parâmetros de segurança, sem o devido credenciamento e autorização, será considerada inadequada e os riscos e potenciais danos serão informados e, caberá ou não, sanção administrativa para o responsável.

DOS DEVERES

Dos Servidores: Considerar as informações do IPESMUC como um bem da entidade, possui grande valor, é um recurso crítico e deve ser tratada de maneira profissional. Devem ser orientados a não circular as informações consideradas confidenciais, e, manter os relatórios e informações armazenadas no local correto.

Dos Prestadores de Serviços: Os prestadores de serviços devem considerar as informações como um bem da entidade, não circular as informações

e/ou mídias confidenciais/restritas, e; é de sua inteira responsabilidade ter conhecimento dessa política, além dos critérios de confidencialidade.

GESTÃO DE RISCOS

A gestão de riscos é um conjunto de ações que visa identificar e implementar medidas de proteção que visam mitigar os riscos quanto a segurança da informação. Algumas ações para mitigar os riscos, são: acompanhamento e auditoria dos conteúdos acessados pelos colaborados; bloqueio de sites suspeitos; bloqueio de sites pornográficos, de jogos, de redes sociais e demais sites que possam apresentar a existência de vírus ou programas maliciosos; Solicitação para *download* de documento/programa de site que não estiver previamente aprovado.

PENALIDADES

Os parâmetros aqui descritos, precisam ser observados com rigor por todos os funcionários do IPESMUC, sendo que, o descumprimento ou inobservância de qualquer uma das diretrizes, caberá medidas administrativas, cíveis e criminais cabíveis ao caso concreto. Ações que caracterizem imprudência, negligência ou imperícia, causando efeitos colaterais com relação a segurança das informações do instituto, serão consideradas infrações disciplinares, gerando medidas administrativas, cíveis e criminais.

DISPOSIÇÕES FINAIS

A política de segurança da informação é um documento a ser seguido por todos os funcionários do instituto, sendo que deve ser apresentada a todos os servidores, prestadores de serviços e demais pessoas que acessem ao instituto.

Além disso, cabe destacar a observância dos processos de controle interno, elencado neste documento como “Gestão de Riscos”, pois, além de mitigar os riscos de vazamento de informações, permite manter os computadores em boas condições de funcionamento e todos os *softwares* em estado de excelência.