INSTITUTO DE PREVIDENCIA SOCIAL DOS SERVIDORES PUBLICOS DO MUNICIPIO DE CAMPO ALEGRE - **IPRECAL**
Avenida Cel. Bento Amorim, 506 – Centro
Campo Alegre–SC adm@iprecal.sc.gov.br
(47) 3632-1574

INSTRUÇÃO NORMATIVA Nº 02, DE 13 DE OUTUBRO DE 2021

INSTITUI E APROVA A POLÍTICA DE SEGURANÇA DE INFORMAÇÃO – PSI, DO INSTITUTO DE PREVIDENCIA SOCIAL DOS SERVIDORES PUBLICOS DO MUNICIPIO DE CAMPO ALEGRE - IPRECAL.

Considerando a aprovação da minuta da **"POLÍTICA DE SEGURANÇA DE INFORMAÇÃO – PSI"** do INSTITUTO DE PREVIDENCIA SOCIAL DOS SERVIDORES PUBLICOS DO MUNICIPIO DE CAMPO ALEGRE – IPRECAL, pelo Conselho Administrativo, em sessão ordinária do dia 29.07.2021;

A Diretora Executiva do Instituto de Previdência Social dos Servidores Públicos de Campo Alegre – IPRECAL, no uso de suas atribuições legais;

RESOLVE:

Art. 1º Instituir e Aprovar a **Política de Segurança da Informação – PSI** do Instituto de Previdência Social dos Servidores Públicos de Campo Alegre – IPRECAL, conforme Anexo Único deste Termo, definida como norma aplicada a todos os Servidores, Conselheiros e Prestadores de Serviços com acesso a informações do IPRECAL, por meio de classificação, permissão e controle de acesso através dos diversos níveis de informação.

Art. 2º Esta Instrução Normativa entra em vigor na data de sua publicação.

Andressa Coelho de Ávila
Andressa Coelho de Ávila
Diretora Executiva do IPRECAL

INSTITUTO DE PREVIDENCIA SOCIAL DOS SERVIDORES PUBLICOS DO MUNICIPIO DE CAMPO ALEGRE - **IPRECAL**
Avenida Cel. Bento Amorim, 506 – Centro
Campo Alegre–SC adm@iprecal.sc.gov.br
(47) 3632-1574

ANEXO ÚNICO
(INSTRUÇÃO NORMATIVA Nº 02, DE 13 DE OUTUBRO DE 2021)

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO - PSI

APRESENTAÇÃO

A Política de Segurança de Informação – PSI no Instituto de Previdência Social dos Servidores do Município de Campo Alegre – IPRECAL, pode ser definida como a adoção de um conjunto de regras e padrões formais que disciplinam e expressam o compromisso dos usuários, possibilitando gerenciar a informação, delimitando o acesso, utilização e disseminação das informações pertencentes ao Instituto, caracterizando as práticas ilícitas e passíveis de punição.

A norma aplica-se a todos os servidores, conselheiros e prestadores de serviço com acesso a informações do IPRECAL, por meio de classificação, permissão e controle de acesso através dos diversos níveis de informação.

1. OS PILARES DA SEGURANÇA DA INFORMAÇÃO

A base da PSI do IPRECAL tomará por preceito 03 pilares fundamentais para a proteção da informação:

Confidencialidade: que é a restrição do acesso a informações somente a pessoas autorizadas, evitando exposição de conteúdo confidencial;

Integridade: que é a precisão, confiabilidade e fidedignidade das informações, evitando alterações indevidas;

Disponibilidade: que consiste em manter a informação primordial sempre acessível.

2. PAPÉIS E RESPONSABILIDADES

Área de Tecnologia de Informação – TI

Avaliar os riscos e propor melhorias na área de segurança da informação, orientar a supervisão/usuários relativo ao uso de tecnologias disponibilizadas, disponibilizar/bloquear o acesso/permissão à rede conforme solicitado pela supervisão do usuário, monitorar e auditar o uso das tecnologias em uso disponibilizadas ao usuário e Efetuar/conferir a realização de *backup* diário.

Servidores, Conselheiros e Prestadores de Serviços

A PSI atinge direta ou indiretamente servidores, conselheiros e prestadores de serviço que possuem acesso a informações de propriedade do Instituto, cabendo-lhes a confidencialidade da informação.

3. CREDENCIAIS E SENHAS

Credencial

A credencial de acesso, contendo o nível de permissões autorizadas poderá a ser modificada conforme a forma de utilização do usuário ou por solicitação do supervisor imediato.

É terminantemente proibido ao usuário:

Instalar programas não licenciados (software pirata);

Remover indevidamente, qualquer arquivo, pasta, *software* ou recurso disponibilizado dentro de suas permissões;

Conectar a rede equipamentos particulares (notebooks, tablets).

Em caso de desligamento do usuário ao Instituto, seus acessos deverão ser imediatamente bloqueados pela área de TI, competindo a supervisão imediata efetuar a solicitação.

Senhas

É de inteira responsabilidade do usuário manter sigilo referente sua senha pessoal de acessos tecnológicos disponibilizados;

4. O USO DOS RECURSOS TECNOLÓGICOS

Os recursos de Tecnologia da Informação englobam todos os equipamentos, periféricos, suprimentos e qualquer outro serviço e/ou dispositivo correlato disponibilizado aos usuários para a realização de atividades diversas, dentre os quais estão incluídos impressoras e suprimentos (papel, tôner, cartuchos de tinta, etc), dispositivos de armazenamento (pendrive, memorycard, CD, DVD, etc), computadores, tablets, celulares, smartphones, contas de acesso (internet, correio eletrônico e demais sistemas), escâneres, rede local, câmeras digitais, etc.

Os recursos tecnológicos são as ferramentas disponibilizadas ao usuário para desempenho de atividades cotidianas referente ao cargo e de exclusivo interesse público, sendo vedada a utilização para fins particulares.

5. DA PERMISSÃO DE ACESSOS

A permissão de acesso ao usuário, bem como os níveis de informação, deverá ser disponibilizada individualmente, com base em suas atividades. A solicitação, alteração e/ou supressão, compete ao supervisor da área.

6. DO ACESSO A REDE LÓGICA DO IPRECAL

Fica terminantemente proibida a conexão de equipamentos particulares na rede do IPRECAL, caracterizando acesso não autorizado, podendo causar falha na segurança.

7. USO DO E-MAIL

A conta de acesso ao e-mail com domínio @iprecal.sc.gov.br é disponibilizada ao usuário para execução de atividades, servindo como instrumento de comunicação com situações relacionadas a suas tarefas cotidianas.

Por padrão, serão bloqueados automaticamente e-mails classificados como perigosos sendo vedada a utilização para fins particulares.

8. USO DA INTERNET

O acesso à internet disponibilizado ao usuário para execução de atividades, serve como instrumento para execução de situações relacionadas a suas tarefas cotidianas relacionadas ao trabalho.

O uso poderá ser Auditado a qualquer momento e, se necessário, bloquear qualquer arquivo, pasta, *site*, correio eletrônico (e-mail particular), aplicação armazenado na rede/internet, estando em rede/disco local ou em áreas privadas da rede.

9. LEI GERAL DE PROTEÇÃO DE DADOS – LGPD (Lei nº 13.709, de 14 de agosto de 2018, alterada pela Lei 13.853, de 08 de julho de 2019).

Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por **pessoa jurídica de direito público** ou privado, com o objetivo de proteger os direitos fundamentais de **liberdade e de privacidade** e o livre desenvolvimento da personalidade da pessoa natural.

Na prática, o ''tratamento de dados'' são operações com dados pessoais, incluídos desde o recolhimento, registro e organização de dados até a consulta e divulgação destas informações. É um processo que permite que empresas recebam pacotes de dados com informações relevantes apenas para elas.

O seu art. 7º nos traz que *"O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:*

I - mediante o fornecimento de consentimento pelo titular;

II - para o cumprimento de obrigação legal ou regulatória pelo controlador;

III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV da Lei;

(...)".

10. USO DE EQUIPAMENTOS PÚBLICOS PARA FINS PARTICULARES.

É terminantemente vedado o uso de equipamentos/recursos de TI para fins particulares como:

- Utilizar a impressora para impressões de material de cunho particular;

- Utilizar a internet (wifi) para downloads de material diverso ao desempenho de seu cargo;

- Armazenar músicas, vídeos, fotos e/ou qualquer material de interesse ou uso pessoal;

- Acessar e-mails particulares utilizando computadores/conexão de internet disponibilizada pelo IPRECAL;

- Acessar através de computadores/conexão de internet disponibilizada pelo IPRECAL, páginas com conteúdo impróprio como pornografia, etc.

11. AUDITORIA E MONITORAMENTO

As atividades na rede passam por um sistema de monitoramento, incluindo e-mail, internet, dispositivos móveis ou wireless e outros componentes de rede. A forma de utilização da rede pelo usuário gera um relatório (LOG de uso), que permite identificar usuário, tempo de acesso e material consultado.

A qualquer tempo, poderá ser realizada pela área de Tecnologia de Informação – TI, Auditoria nos recursos tecnológicos disponibilizados, sem aviso prévio ou mesmo permissão/consentimento do usuário.

12. BACKUP

Backup é uma cópia de segurança de dados, com objetivo de resguardar informações de uma eventual perda de arquivos. Deve ser executado com de forma automática com periodicidade diária.

13. SANSÕES

Não poderá o servidor e/ou prestador de serviços alegar o desconhecimento da PSI, a infração a norma editada poderá causar sanções, conforme deveres dos servidores municipais previstos no Estatuto dos Servidores do Município de Campo Alegre, LCM 06/2002, Art. 207 e 208.

14. DISPOSIÇÕES FINAIS

Esta Política de Segurança de Informação – PSI visa a uniformização de processos e procedimentos referente ao uso dos recursos de TI disponibilizados aos servidores municipais.

Esta normativa entra e vigor na data de sua publicação.

Andressa Coelho de Ávila

Andressa Coelho de Ávila
Diretora Executiva do IPRECAL