DECRETO Nº 13.663, DE 07/08/2024

Dispõe sobre a segurança de dados e informações no âmbito da Administração Direta do Poder Executivo.

O Prefeito Municipal de Ponte Nova, no uso de suas atribuições e considerando a necessidade de instituir mecanismos de proteção e controle do uso e do armazenamento de dados e informações nas diversas unidades administrativas, decreta:

Art. 1º Este decreto institui procedimentos básicos a serem seguidos em todas as unidades da Prefeitura de Ponte Nova no uso de dispositivos fixos e móveis de produção, armazenamento e transferência de dados e informações internamente ou com usuários externos.

Art. 2º As senhas pessoais não devem ser compartilhadas com ninguém, ainda que se trate de colega de trabalho, e devem ser ou memorizadas ou armazenadas em local seguro e inacessível a terceiros, nunca devendo ser enviadas em mensagens de qualquer tipo.

Parágrafo único. Devem ser evitadas senhas óbvias como datas de aniversário ou sequências simples e as senhas devem ser substituídas regularmente para evitar vazamentos.

Art. 3º E-mails suspeitos ou de remetentes desconhecidos não devem ser abertos em nenhuma hipótese assim como não se deve clicar em links ou fazer downloads de seus anexos, devendo-se sempre consultar a área de tecnologia de informação em caso de dúvidas.

Art. 4º A navegação na internet deve ficar restrita a páginas relacionadas ao trabalho não sendo permitido o acesso a *sites* de *streaming*, como Netflix, Globo Play e Star+, ou a plataformas de vídeos online, como Youtube ou Vimeo, a menos de busca de informações necessárias ao trabalho em vídeos instrutivos.

Art. 5º As redes sem fio (*Wi-Fi*) do Município não devem ser usadas para fins particulares, pois podem causar falhas de segurança e consumo desnecessário de banda de internet.

Art. 6º A utilização de dispositivos de armazenamento externo deve ser precedida de verificação de segurança junto à área de Tecnologia de Informação, não se devendo conectar dispositivos USB desconhecidos ao computador.

Parágrafo único. Em caso de necessidade de compartilhamento de arquivos deve-se dar preferência ao *e-mail*, meio mais seguro por requerer autenticação e diminuir os riscos de contaminação dos equipamentos quando proveniente de fontes seguras.

Art. 7º O computador de uso pessoal deve ser acessado por senha e deve ser mantido bloqueado sempre que o usuário se afaste, mesmo que por pouco tempo.

Parágrafo único. A senha utilizada pelo usuário deve ser informada à chefia imediata para acesso em caso de ausências ou fatalidade, todavia não deve ser repassada a outras pessoas, servidores ou não, sem o conhecimento ou autorização da chefia imediata.

Art. 8º Dispositivos móveis não devem ser deixados sem vigilância em locais públicos e salas de uso privativo devem ser fechadas com chave na ausência do usuário para evitar acessos não autorizados**.**

Art. 9º Documentos importantes devem ficar arquivados e adequadamente protegidos, a salvo de acesso por pessoas estranhas ao serviço.

Art. 10. Não se deve compartilhar informações sensíveis ou dados pessoais de usuários ou servidores sem autorização documentada da Administração.

Art. 11. O uso de redes sociais relacionadas ao trabalho deve ser feito com a necessária cautela e prudência para evitar postagens inadequadas, assim como de informações sensíveis ou comprometedoras.

Art. 12. O usuário deve fazer regularmente cópias de segurança (*back-ups*) de arquivos importantes, em locais seguros, fora de seu dispositivo de trabalho, como armazenamento em nuvem (Google Drive, One Drive, Dropbox) e dispositivos portáteis (HDs externos e pendrives).

Parágrafo único. Devem ser providenciadas duas ou mais formas de *back-ups* para garantia de segurança e no caso de dúvidas o usuário deve procurar a área de Tecnologia de Informação pelo telefone (31) 3819-5459 ou pela plataforma 1Doc, no menu de Protocolo.

Art. 13. O usuário deve procurar se cientificar das informações sobre segurança e segui-las adequadamente, relatando imediatamente à área de Tecnologia da Informação qualquer atividade que considere suspeita, assim como perda ou extravio de dispositivo.

Art. 14. A área de Tecnologia de Informação deve ser informada sobre admissões, exonerações, transferências e outras formas de ingresso e saída de usuários em cada unidade, para que as permissões de uso dos sistemas do Município sejam concedidas e revogadas.

Art. 15. A utilização dos equipamentos de informática por pessoas não autorizadas, seja servidor ou não, ou para fins não relacionados ao exercício da função, é passível de sanções, nos termos do Estatuto do Servidor Público.

Art. 16. Este Decreto entra em vigor na data de sua publicação.

Art. 17. Revogam-se as disposições contrárias.

Ponte Nova, 07 de agosto de 2024.

Wagner Mol Guimarães
Prefeito Municipal

Afonso Mauro Pinho Ribeiro
Secretário Municipal de Planejamento e Desenvolvimento Econômico