DECRETO N° 1619, DE 11 DE JUNHO DE 2025.

"DISPÕE SOBRE A CRIAÇÃO DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO (POSIN)"

EBER ROGERIO ASSIS, PREFEITO MUNICIPAL DE FERNÃO, ESTADO DE SÃO PAULO NO USO DE DUAS ATRIBUIÇÕES,

CONSIDERANDO a necessidade de instituir a Política de Segurança da Informação (POSIN) no âmbito da administração pública municipal.

DECRETA:

Art. 1° - Fica instituída a Política de Segurança da Informação (POSIN) nos órgãos e nas entidades da Administração Pública Municipal, que tem como pressupostos básicos:

I – Confidencialidade: Garantir que as informações não estejam acessíveis ou reveladas a pessoas físicas, sistemas, órgãos ou entidades não autorizadas ou credenciadas;

II – Integridade: Garantir que as informações contidas nos recursos tecnológicos não sejam alteradas indevidamente ou destruídas de maneira não autorizada, seja intencionalmente ou acidentalmente;

III - Disponibilidade: Garantir que as informações estejam acessíveis e em condições de serem utilizadas por usuários ou custodiantes autorizados.

Art. 2.° - Para efeitos da Política de Segurança da Informação, ficam estabelecidas as seguintes conceituações:

I - Auditoria: Verificação e avaliação dos sistemas e procedimentos internos com o objetivo de reduzir fraudes, erros, práticas ineficientes ou ineficazes;

II - Não-repúdio: Utilizado para garantir que os usuários não possam negar uma ação ou operação de sua autoria;

III - Plano de Continuidade de Negócios (PCN): Aplicação de estratégias capazes de realizar a continuidade durante a disrupção, prontidão para continuidade e retomada de recursos em momentos de crise, evitando falhas catastróficas em processos críticos da instituição;

IV - Recursos de Tecnologia da Informação e Comunicação ou simplesmente "Recursos de TIC": Ativos de *hardware*, *software*, serviços de conexão e comunicação ou infraestrutura física necessárias para criação, registro, armazenamento, manuseio, transporte, compartilhamento e descarte de informações;

V - Segurança da Informação (SI): Preservação da confidencialidade, integridade, disponibilidade da informação. Visa proteger a informação contra ameaças para garantir a continuidade dos negócios, minimizar danos e maximizar o retorno sobre investimentos e novas oportunidades de transação.

Art. 3.° - São diretrizes básicas da Política de Segurança da Informação:

I - Definir os padrões de implementação efetiva da segurança da informação, garantindo a proteção de dados em meios físicos e digitais atenção as melhores práticas estabelecidas pelas normas ABNT NBR ISO/IEC 27001 (Segurança da informação, segurança cibernética e proteção à privacidade - Sistemas de gestão da segurança da informação - Requisitos) e ABNT NBR ISO/IEC 27002 (Segurança da informação, segurança cibernética e proteção à privacidade - Controles de segurança da informação);

II - Orientar os colaboradores da Prefeitura de Municipal de Fernão a adotarem comportamentos alinhados com as necessidades do negócio e os requisitos legais de privacidade e proteção de dados pessoais;

III - Promover ações para a manutenção da segurança da informação, criando normas específicas para sistemas de informação e assegurando a eficácia dos controles e processos estabelecidos;

IV - Manter todos os mecanismos de proteção para assegurar a segurança da informação, visando a continuidade no órgão;

V - Considerar toda informação gerada por colaboradores, utilizando recursos da Prefeitura, como propriedade do órgão;

VI - Reavaliar periodicamente as ameaças e riscos para assegurar a proteção do órgão;

VII - Restringir o acesso às informações produzidas ou recebidas às atribuições necessárias para o desempenho das atividades dos usuários;

VIII - Alinhar os processos de aquisição ou contratação de bens e serviços de tecnologia da informação com a POSIN e seus documentos auxiliares, em conformidade com a legislação vigente;

IX - Utilizar os equipamentos de informática e comunicação, sistemas e informações exclusivamente para o cumprimento das atividades profissionais;

X - Revisar e ajustar a POSIN periodicamente, sempre que ocorrerem eventos ou fatos relevantes;

XI - Evitar a circulação de informações e/ou mídias confidenciais e assegurar que relatórios não sejam deixados em locais de fácil acesso;

XII - Aderir ao conceito de "mesa limpa", garantindo que, ao concluir o trabalho, não haja relatórios e/ou mídias confidenciais sobre as mesas;

XIII - Executar os procedimentos de gestão de continuidade do negócio em conformidade com os requisitos de segurança da informação da Prefeitura.

Artigo 4° - Para fins deste Decreto, serão adotadas as seguintes regras:

I - Assegurar que todos os mecanismos de proteção à segurança da informação sejam mantidos e que toda informação gerada seja considerada propriedade do órgão;

II - Reavaliar periodicamente as ameaças e riscos, garantindo que o acesso às informações seja restrito conforme as necessidades do desempenho das atividades;

III - Alinhar os processos de aquisição ou contratação de bens e serviços de tecnologia com a Política de Segurança da Informação e utilizar equipamentos e sistemas exclusivamente para atividades profissionais;

IV - Revisar e ajustar a Política de Segurança da Informação conforme eventos relevantes, evitando a circulação indevida de informações confidenciais e assegurando a prática de "mesa limpa";

V - Executar procedimentos de Continuidade do Negócio em conformidade com os requisitos de segurança da informação e permitir que o acesso à rede seja exclusivo e intransferível, sendo o usuário responsável por suas atividades;

VI - Restringir o acesso a Recursos de TIC a colaboradores autorizados e implementar controles de acesso físico para proteger dados e arquivos da prefeitura;

VII - Limitar o uso da internet a fins profissionais e possibilitar que os equipamentos e serviços de acesso sejam propriedade do órgão, com medidas de bloqueio de conteúdo impróprio**;**

VIII - Responsabilizar os colaboradores por suas ações na internet e restringir o uso de proxies, VPNs, e conteúdo não relacionados ao trabalho;

IX - Proibir alterações físicas em equipamentos de informática e propiciar que qualquer dano ou extravio seja comunicado imediatamente ao setor responsável;

X - Limitar o uso do e-mail corporativo a finalidades institucionais e proteger o acesso com senhas seguras, evitando a divulgação e o uso inadequado;

XI - Responsabilizar cada colaborador pelo *backup* e organização de seus arquivos, garantindo o armazenamento adequado no servidor;

XII - Classificar as informações conforme seu nível de confidencialidade, estabelecendo critérios claros para cada área do órgão.

Artigo 5° - Instituído o Comitê de Privacidade de Segurança da Informação e Privacidade (CSIP), caberão as seguintes atribuições:

I - Avaliar os mecanismos atuais de tratamento e proteção de dados pessoais no âmbito da prefeitura, propondo políticas, estratégias e metas que assegurem a conformidade operacional da Controladora com as disposições da Lei n.º 13.709/2018 (Lei Geral de Proteção De Dados - LGPD);

II - Analisar assuntos relacionados à Segurança da Informação em atenção as melhores práticas estabelecidas pelas normas ABNT NBR ISO/IEC 27001 (Segurança da informação, segurança cibernética e proteção à privacidade - Sistemas de gestão da segurança da informação - Requisitos) e ABNT NBR ISO/IEC 27002 (Segurança da informação, segurança cibernética e proteção à privacidade - Controles de segurança da informação);

III - Propor princípios, diretrizes e regras para a gestão de dados pessoais;

IV - Propor políticas, procedimentos e planos para regulamentar a gestão de dados pessoais pelos agentes internos e externos que tratam dados pessoais em nome do controlador ou em função do cumprimento do contrato firmado com o controlador;

V - Prestar orientações sobre o tratamento e a proteção de dados pessoais de acordo com as diretrizes estabelecidas na LGPD e documentos internos sobre o tema;

VI - Promover a comunicação interna e externa acerca das medidas de proteção de dados adotadas, de ofício ou mediante provocação do interessado pessoais outros órgãos;

VII - Auxiliar o(a) Encarregado(a) de Dados na auditoria do tratamento realizado pelos operadores de dados pessoais;

VIII - Sugerir sanções administrativas quando houver violação às políticas pré-estabelecidas;

IX - Auxiliar nos trabalhos do(a) Encarregado(a) de Dados, garantindo-lhe a autonomia necessária ao exercício do seu encargo legal.

Parágrafo único. O funcionamento e as atribuições do Comitê de Segurança da Informação e Privacidade (CSIP) serão regulados em decreto específico.

Artigo 6° - Este Decreto entra em vigor na data de sua publicação.

Prefeitura Municipal de Fernão, 11 de junho de 2025.

EBER ROGERIO ASSIS:27657319852

Assinado de forma digital por EBER ROGERIO ASSIS:27657319852
Dados: 2025.06.11 09:59:58 -03'00'

Eber Rogério Assis
RG n° 25.921.496-6
Prefeito Municipal

Registrado e Publicado por afixação no Saguão da Prefeitura Municipal de Fernão, em local próprio – Data Supra