DECRETO Nº 5.471, DE 9 DE DEZEMBRO DE 2021.

Institui a Política de Segurança da Informação no âmbito da Administração Direta e Indireta do Município de Vargem Grande do Sul, e dá outras providências.

O Prefeito Municipal de Vargem Grande do Sul, Estado de São Paulo, no uso de suas atribuições legais,

CONSIDERANDO a necessidade de normatizar o uso apropriado dos recursos da tecnologia da informação no âmbito da Administração Direta e Indireta do Município de Vargem Grande do Sul, promovendo a proteção dos usuários, dos equipamentos, dos softwares, dos dados dos contribuintes e da própria Administração Pública;

CONSIDERANDO que a Política de Segurança da Informação tem como objetivo garantir a correta e adequada utilização dos recursos de informática como a internet, intranet, ativos e manuseio das informações institucionais veiculadas, bem como assegurar padrões satisfatórios de qualidade na prestação do serviço de tecnologia da informação da Administração Direta e Indireta no Município de Vargem Grande do Sul, fazendo-se, pois, necessária a especificação de uma política de utilização dos recursos tecnológicos a ele vinculados;

CONSIDERANDO a necessidade de garantir a segurança das informações geradas, adquiridas, processadas, armazenadas e transmitidas no âmbito da Administração Municipal, de forma a atender aos princípios da confidencialidade, integridade, disponibilidade, autenticidade e legalidade;

CONSIDERANDO que os servidores públicos municipais devem zelar pelas informações que lhes são confiadas no exercício de suas funções;

CONSIDERANDO que as consequências geradas pela violação de quaisquer dos deveres dispostos neste decreto ficam sob inteira responsabilidade do servidor público municipal ou convidado, e que qualquer ato ilícito ou danoso, praticado pelos recursos computacionais disponibilizados que venham a causar prejuízos ou danos às informações ou sistemas de uso diário ou prejudicando a imagem da Administração Direta e Indireta no Município de Vargem Grande do Sul, serão submetidos a sanções disciplinares ou punitivas correspondentes à gravidade do ato;

CONSIDERANDO que as ações de segurança da informação reduzem custos e riscos e aumentam os benefícios disponibilizados aos cidadãos, ao permitir a oferta de processos, produtos e serviços suportados por sistemas de informações mais seguros;

DECRETA:

Art. 1º Fica instituída a Política de Segurança da Informação no âmbito da Administração Direta e Indireta do Município de Vargem Grande do Sul.

§ 1º A Política de Segurança da Informação constitui um conjunto de diretrizes e normas que estabelecem o princípio de proteção, controle e monitoramento das informações processadas, armazenadas e custodiadas pela Administração Direta e Indireta Municipal, aplicando-se a todos os órgãos do Poder Executivo Municipal.

§ 2º Compete ao Departamento de Administração, por intermédio da Divisão de Processamento de Dados e Informática, a coordenação das políticas de gestão da segurança da informação no Município.

Art. 2º Para efeito deste Decreto ficam estabelecidos os seguintes conceitos:

I - autenticidade: garantia que a informação é procedente e fidedigna, capaz de gerar evidências não repudiáveis da identificação de quem a criou, editou ou emitiu;

II - confidencialidade: garantia de que as informações sejam acessadas e reveladas somente a indivíduos, órgãos, entidades e processos devidamente autorizados;

III - dado: parte elementar da estrutura do conhecimento, computável, mas, incapaz de, por si só, gerar conclusões inteligíveis ao destinatário;

IV - disponibilidade: garantia de que as informações e os recursos de tecnologia da informação estejam disponíveis sempre que necessário e mediante a devida autorização para seu acesso ou uso;

V - gestor da informação: pessoa detentora de competência institucional para autorizar ou negar acesso à determinada informação ao usuário;

VI - incidente de segurança da informação: um evento ou uma série de eventos de segurança da informação indesejados ou inesperados, que tenham uma grande probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação (ISO/ IEC 27001);

VII - informação: conjunto de dados que, processados ou não, podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;

VIII - integridade: garantia de que as informações estejam protegidas contra manipulações e alterações indevidas;

IX - legalidade: garantia de que todas as informações sejam criadas e gerenciadas de acordo com a legislação em vigor;

X - log: registro de atividades gerado por programa de computador que possibilita a reconstrução, revisão e análise das operações, procedimento ou evento em sistemas de informação;

XI - não repúdio: garantia de que um usuário não consiga negar uma operação ou serviço que modificou ou criou uma informação;

XII - recursos da tecnologia da informação: recursos físicos e lógicos utilizados para criar, armazenar, manusear, transportar, compartilhar e descartar a informação, dentre estes podemos destacar os computadores, notebooks, tablets, pendrives, mídias, impressoras, scanners, softwares, etc.;

XIII - risco: combinação de probabilidades da concretização de uma ameaça e seus potenciais impactos;

XIV - segurança da informação: preservação da confidencialidade, integridade e disponibilidade da informação; adicionalmente, outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confiabilidade, podem também estar envolvidas (ISO/ IEC 27001);

XV - senha: conjunto alfanumérico de caracteres destinado a assegurar a identidade do usuário e permitir seu nível de acesso aos recursos da tecnologia da informação não disponíveis ao público, de uso pessoal e intransferível;

XVI - tecnologia da informação e comunicação: solução ou conjunto de soluções sistematizadas baseadas no uso de recursos tecnológicos que visam resolver problemas relativos à geração, tratamento, processamento, armazenamento, veiculação e reprodução de dados, bem como subsidiar processos que convertem dados em informação;

XVII - usuário: servidor, comissionado, empregado, estagiário, prestador de serviço, terceirizado, conveniado, credenciado, fornecedor ou qualquer outro indivíduo ou organização que venham a ter relacionamento, direta ou indireta, com os órgãos e entidades da Administração Municipal;

XVIII - violação: qualquer atividade que desrespeite as diretrizes estabelecidas nesta política ou em quaisquer das demais normas que a complemente.

Art. 3º Constituem objetivos da Política de Segurança da Informação:

I - dotar a Administração Direta e Indireta do Município de Vargem Grande do Sul de instrumento jurídico, normativo e institucional que a capacite de forma técnica e administrativa, com o objetivo de assegurar a confidencialidade, a integridade, a autenticidade, o não repúdio e a disponibilidade dos dados e das informações tratadas, classificadas e sigilosas da Administração Municipal;

II - estabelecer e controlar os níveis de acesso de fornecedores externos aos sistemas, equipamentos, dispositivos e atividades vinculadas à segurança dos sistemas de informação;

III - assegurar a interoperabilidade entre os sistemas de segurança da informação;

IV - incorporação da cultura da segurança da informação, por todos os usuários, como um elemento essencial em seus hábitos e atitudes dentro e fora da organização.

Art. 4º A Política de Segurança da Informação instituída neste Decreto reger-se-á pelos seguintes princípios:

I - tratamento da informação como patrimônio, tendo em vista que a divulgação das informações estratégicas de qualquer natureza pertencentes à Administração Pública deve ser protegida de forma adequada, com vistas a evitar alterações, acessos ou destruição indevidos;

II - classificação da informação, garantindo-lhe o adequado nível de proteção, considerando:

a) a avaliação da necessidade do tipo de acesso pelo usuário, adotando-se como parâmetro o grau de confidencialidade da informação;

b) a definição de confidencialidade da informação em consonância com as atividades desempenhadas pelo usuário, com vistas a garantir a adequada autorização de acesso pelo gestor da informação, que deverá conter os limites de acesso, tais como leitura, atualização, criação e remoção, entre outros.

III - controle de acesso às informações, tendo como orientação a classificação definida no inciso II deste artigo, respeitando a legislação vigente e considerando, ainda, que:

a) o acesso e o uso de qualquer informação, pelo usuário, deve se restringir ao necessário para o desempenho de suas atividades;

b) no caso de acesso a sistemas informatizados, deverão ser utilizados sistemas e tecnologias autorizados pela Administração;

IV - continuidade do uso da informação, sendo necessária, para o funcionamento dos sistemas, pelo menos uma cópia de segurança atualizada e guardada em local remoto, com nível de proteção equivalente ao nível de proteção da informação original, observada as seguintes regras:

a) para a definição das cópias de segurança, devem ser considerados os aspectos legais, históricos, de auditoria e de recuperação de ambiente;

b) os recursos tecnológicos, de infraestrutura e os ambientes físicos utilizados para suportar os sistemas de informação devem ter controle de acesso físico, condições ambientais adequadas e ser protegidos contra situações de indisponibilidade causadas por desastres ou contingências;

c) definição do nível de disponibilidade para cada serviço prestado pelos sistemas de informação, nas situações mencionadas na alínea "b" deste inciso.

V - educação em segurança da informação, devendo ser observado pelo usuário a correta utilização das informações e dos recursos computacionais disponibilizados.

Art. 5° As medidas a serem adotadas para fins de proteção da informação deverão considerar:

I - os níveis adequados de integridade, confidencialidade e disponibilidade da informação;

II - a compatibilidade entre a medida de proteção e o valor do ativo protegido;

III - o alinhamento com as diretrizes da Administração Municipal;

IV - as melhores práticas para a gestão da segurança da informação;

V - os aspectos comportamentais e tecnológicos apropriados.

Art. 6° Compete à Divisão de Processamento de Dados e Informática:

I - elaborar e revisar continuamente os procedimentos e a normatização relacionada ao processo de gestão da segurança da informação;

II - avaliar propostas de modificação da Política de Segurança da Informação encaminhadas pelos demais órgãos administrativos da Administração Direta e Indireta Municipal;

III- planejar, elaborar e propor estratégias e ações para institucionalização da política, normas e procedimentos relativos à segurança da informação;

IV - avaliar a eficácia dos procedimentos relacionados à segurança da informação, propondo e implementando medidas que visem à melhoria do processo de gestão da segurança da informação no âmbito da Administração Municipal;

V - apurar os incidentes de segurança críticos e dar o encaminhamento adequado;

VI - promover a conscientização, o treinamento e a educação em segurança da informação.

VII - subsidiar o processo de classificação da informação, de forma a viabilizar a correta definição a ela relacionada;

VIII - responsabilizar-se pela exatidão, integridade e atualização da informação sob sua custódia;

IX - subsidiar na compatibilização de estratégias, planos e ações desenvolvidos no âmbito da Administração Municipal relativos à segurança da informação;

X - realizar análise de riscos em processos, em consonância com os objetivos e ações estratégicas estabelecidas pelo Poder Executivo e atualizá-la periodicamente;

XI - relatar os incidentes de segurança da informação para que sejam tomadas as devidas providências em conjunto com as áreas diretamente envolvidas.

Art. 7° Ao perder o vínculo com a Administração Direta e Indireta Municipal, todos os acessos do usuário aos recursos da tecnologia da informação serão excluídos, suas contas de e-mails canceladas e seu conteúdo apagado.

§ 1°. Fica a Divisão de Recursos Humanos, responsável por repassar à Divisão de Processamento de Dados e Informática, a qualquer tempo, as demissões/exonerações, do quadro de servidores/empregados, para que as providências acima sejam tomadas.

§ 2º. Ficam, os demais Departamentos e órgãos municipais, responsáveis por repassar à Divisão de Processamento de Dados e Informática, a qualquer tempo, os encerramentos contratuais com estagiários, prestadores de serviço, terceirizados, conveniados, credenciados, fornecedores ou qualquer outro indivíduo ou organização que venham a ter relacionamento, direta ou indireta com a municipalidade, para que as providências acima sejam tomadas.

Art. 8º É dever do usuário, em consonância com a Política de Segurança da Informação estabelecida neste Decreto:

I - zelar pelo sigilo da sua senha;

II - zelar pela segurança das informações, fechando ou bloqueando o acesso aos equipamentos de informática ou softwares quando não estiver utilizando;

III - comunicar imediatamente ao seu superior hierárquico qualquer suspeita de que estejam sendo executados atos em seu nome por meio dos recursos da tecnologia da informação;

IV - zelar pela integridade física dos equipamentos de informática utilizados, evitando submetê-los a condições de riscos, mantendo-os afastados de líquidos e alimentos, não danificando as placas de patrimônio, não colando qualquer tipo de adesivo nos equipamentos ou qualquer material e/ ou utensílio que possa danificá-los, comunicando ao órgão competente qualquer anormalidade ou defeito;

V - zelar pela segurança da informação que esteja sob sua custódia em razão de seu exercício funcional.

Art. 9º É proibido aos usuários:

I - fornecer por qualquer motivo, seu login e senha para acesso a outrem;

II - fazer uso do login e da senha de terceiro;

III - utilizar os recursos da tecnologia da informação em desacordo com os princípios éticos da Administração Pública;

IV - visualizar, acessar, expor, armazenar, distribuir, editar ou gravar material de natureza pornográfica, racista, criminosa, jogos, música, filmes e outros relacionados, por meio de uso de recursos de equipamentos da Administração Direta e Indireta Municipal;

V - acessar sites ou serviços que representem risco aos dados ou à estrutura de redes da Administração Direta e Indireta Municipal;

VI - fazer cópias não autorizadas dos softwares desenvolvidos ou adquiridos pela Administração Direta e Indireta Municipal.

Art. 10. É vedado o uso de equipamentos de informática particulares conectados à rede de informática da Administração Direta e Indireta Municipal, sem a prévia autorização da Divisão de Processamento de Dados e Informática.

Art. 11. São considerados usos inadequados dos equipamentos de informática:

I - instalar hardware em equipamentos de informática da Administração Direta e Indireta Municipal;

II - instalar softwares de qualquer espécie em equipamentos de informática da Administração Direta e Indireta Municipal;

III - reconfigurar a rede corporativa ou inicializá-la sem prévia autorização expressa;

IV - efetuar montagem, alteração, conserto ou manutenção em equipamentos da Administração Direta e Indireta Municipal sem o conhecimento da Divisão de Processamento de Dados e Informática;

V - alterar o local de instalação dos equipamentos/hardwares de informática, sem prévia autorização;

VI - instalar dispositivo ou utilizar internet móvel, sem prévia autorização expressa;

VII - utilizar mecanismos para burlar o usuário/administrador, concedendo privilégios aos demais usuários;

VIII - utilizar dispositivos de armazenamento externos tais como pen drive, HD externo, sem prévia autorização;

Art. 12. Compete exclusivamente à Divisão de Processamento de Dados e Informática realizar backup diário dos dados armazenados nos servidores internos da Administração Direta e Indireta Municipal.

Parágrafo único. Não compete à Divisão de Processamento de Dados e Informática fazer backup diário ou periódico de informações armazenadas localmente nos computadores, porém, aquela deverá orientar os usuários quanto às melhores práticas para realização de backups para aplicativos instalados em computadores locais e quanto à importância de salvar os arquivos mais importantes na rede municipal.

Art. 13. A Administração Direta e Indireta Municipal adotará política interna de inspeção e restrição de acesso à internet, com a identificação do usuário por meio de sistema automatizado.

Art. 14. É considerado uso inadequado da internet:

I - acessar informações consideradas inadequadas ou não relacionadas às atividades administrativas, especialmente sites de conteúdo agressivo/criminoso (racismo, pedofilia, nazismo, etc.), de drogas, pornografia e outros relacionados;

II - fazer download de arquivos e outros que possam tornar a rede local vulnerável a invasões externas e ataques a programas de código malicioso em suas diferentes formas;

III - violar os sistemas de segurança da Administração Direta e Indireta Municipal;

IV - tentar ou efetivamente burlar as regras definidas de acesso à internet;

V - alterar os registros de acesso à internet;

VI - realizar ataque ou invadir computadores da Administração Direta e Indireta Municipal;

VII - utilizar acesso à internet provido pela Administração Direta e Indireta Municipal para transferência de arquivos que não estejam relacionados às suas atividades;

VIII - divulgar informações confidenciais da Administração Direta e Indireta Municipal em grupos de discussão, listas ou bate-papos, não importando se a divulgação foi deliberada ou inadvertida, sendo possível sofrer as penalidades previstas na forma da lei.

Art. 15. O chefe imediato do usuário deverá comunicar quaisquer ações que comprometam a segurança, a integridade, o desempenho e a descaracterização de equipamentos e redes da Administração Direta e Indireta Municipal.

Art. 16. O usuário, a critério de seu chefe imediato e de acordo com as necessidades do serviço, poderá ter acesso a uma conta de correio eletrônico.

Art. 17. Os usos de softwares de compartilhamento de arquivos e de troca de mensagens serão tratados em Decreto específico.

Art. 18. Todo caso de exceção às determinações da Política de Segurança da Informação deve ser analisado de forma individual, aplicável apenas ao seu solicitante, dentro dos limites e motivos que o fundamentaram.

Art. 19. A não observância da Política de Segurança da Informação pelos usuários configura descumprimento de dever funcional, indisciplina e/ou insubordinação, conforme o caso, sujeitando o infrator à incidência das sanções cabíveis, nos termos da legislação vigente.

Art. 20. Este Decreto entra em vigor na data de sua publicação.

Art. 21. Revogam-se as disposições em contrário.

Vargem Grande do Sul, 9 de dezembro de 2021.

AMARILDO DUZI MORAES

Registrado e publicado na Secretaria Geral da Prefeitura Municipal de Vargem Grande do Sul, Estado de São Paulo, em 9 de dezembro de 2021.

GUILHERME MANSARA LOPES DA SILVA
Assinando por delegação, conforme Portaria nº 18.534, de 19 de março de 2021.