DECRETO Nº 3.754/2024

de 14 de novembro de 2024.

"Institui a Política de Segurança da Informação no âmbito da Prefeitura do Município de Capela do Alto e dá outras providências".

PÉRICLES GONÇALVES, Prefeito do Município de Capela do Alto, no uso de suas atribuições legais,

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

CONSIDERANDO o que é estabelecido pela Lei Geral de Proteção de Dados - LGPD, LEI 13.709 de 14 de agosto de 2018;

CONSIDERANDO o Decreto Municipal 3.526 de 24 de maio de 2023 que regulamenta a aplicação da Lei Federal nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais - LGPD), no âmbito do Poder Executivo do Município de Capela do Alto, cria o Comitê Gestor de Governança de Dados e Informações (CGGDI) e dá outras providências, bem como a Portaria nº 231, de 01 de junho de 2023 que regula e Institui o Comitê Gestor de Governança de Dados e Informações (CGGDI);

CONSIDERANDO a necessidade de normatizar o uso apropriado dos recursos da tecnologia da informação no âmbito da Prefeitura do Município de Capela do Alto, promovendo a proteção dos usuários, dos equipamentos, dos softwares, dos dados dos contribuintes e da própria Administração Pública Municipal;

CONSIDERANDO que a falta, falha ou mau uso desse serviço poderá causar graves danos à Administração Pública Municipal;

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

D E C R E T A:

Art. 1º Fica instituída a Política de Segurança da Informação no âmbito da Prefeitura do Município de Capela do Alto.

§ 1º A Política de Segurança da Informação constitui um conjunto de diretrizes, normas e procedimentos que estabelecem o princípio de proteção, controle e

monitoramento das informações processadas, armazenadas e custodiadas pela Administração Municipal, aplicando-se a todos os órgãos do Poder Executivo Municipal.

§ 2º A Política é destinada a todos servidores/as públicos da Administração Pública da Prefeitura de Capela do Alto, devendo os mesmos atentar-se para o cumprimento das normas e procedimentos aqui estabelecidos, integralmente, conforme o descrito nos artigos subsequentes.

§ 3º Compete ao Departamento de Tecnologia da Informação a coordenação das políticas de gestão da segurança da informação no Município em conjunto a atuação do Comitê Gestor de Governança de Dados e Informações (CGGDI).

§ 4º Compete ao Departamento de Tecnologia da Informação a execução de atividades específicas da área que lhe são conferidas nos artigos subsequentes.

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

I – 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, smartphones, etc;

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

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

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

V – 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;

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

VII - 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);

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

IX – integridade: garantia de que as informações estejam protegidas contra manipulações e alterações indevidas;

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

XI – login ou ID de usuário: identificação única do usuário, permitindo o seu acesso e controle na utilização dos recursos da tecnologia da informação;

XII - 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;

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

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

XV - 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);

XVI – 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;

XVII – 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;

XVIII – usuário: funcionário, servidor, comissionado, 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;

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

XX - interoperabilidade: refere-se à capacidade de sistemas, dispositivos ou entidades diferentes se comunicarem, compartilharem dados e interagirem entre si de forma eficaz e sem ambiguidades. Isso geralmente implica a capacidade de diferentes sistemas entenderem e utilizarem os mesmos padrões, protocolos e formatos de dados, permitindo uma troca de informações fluida e eficiente. A interoperabilidade é fundamental em muitos campos, como tecnologia da informação, saúde, transporte e governança, facilitando a integração e a colaboração entre diferentes partes e sistemas.

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

I – dotar a Prefeitura do Município de Capela do Alto 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;

V – definir e determinar responsáveis dentro da Administração Pública (setorialmente e também integralmente) pelo estabelecimento de procedimentos, pelo monitoramento e pelo cumprimento dos mesmos.

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 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 autorizadas pela Administração, por meio de usuário e senha, ambos pessoais e intransferíveis.

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, observadas as seguintes regras e procedimentos:

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 e procedimentos 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 ao Departamento de Tecnologia da Informação, supervisionada pela Diretoria Municipal da Administração:

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 Municipal;

III – garantir que os registros de auditoria de eventos de segurança da informação sejam produzidos e mantidos em conformidade com as normas vigentes;

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

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

VI – apurar os incidentes de segurança críticos e dar o encaminhamento adequado;

VII – promover a conscientização, o treinamento e a educação em segurança da informação.

Art. 7° Compete aos membros do Comitê Gestor de Governança de Dados e Informações (CGGDI), complementarmente às demais diretrizes estabelecidas neste Decreto:

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

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

III – subsidiar o Departamento de Tecnologia da Informação na compatibilização de estratégias, planos e ações desenvolvidos no âmbito da Administração Municipal relativos a segurança da informação;

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

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

Art. 8º O Departamento de Tecnologia da Informação é a única detentora e responsável pela senha de administrador dos equipamentos.

Parágrafo único. As solicitações para compartilhamento da senha de administrador dos equipamentos deverão ser encaminhadas com a devida justificativa para que seja avaliada esta necessidade em conjunto com o órgão solicitante.

Art. 9º Compete exclusivamente ao Departamento de Tecnologia da Informação realizar backup diário dos dados armazenados nos servidores internos da Prefeitura e fiscalizar como está sendo realizado o backup dos servidores armazenados nos servidores externos.

§ 1º. A Política de Backup está descrita no Anexo IV, do presente decreto, conforme disposto no art. 46 da Lei Federal nº 13.709/2018.

§ 2º. É de responsabilidade do Departamento de Tecnologia da Informação, o planejamento, execução, validação e atualização da Política de Backup.

§ 3º. Não compete à Departamento de Tecnologia da Informação fazer backup diário ou periódico de informações armazenadas localmente nos computadores, porém, a mesma deverá orientar os usuários quanto às melhores práticas para realização de backups para aplicativos instalados em computadores locais e quanto a importância de salvar os arquivos mais importantes na rede da Prefeitura.

Art. 10. O cadastro, habilitação e inabilitação de usuário para acesso aos recursos da tecnologia da informação, depende de prévio encaminhamento do formulário constante no Anexo II deste Decreto, autorizado pela chefia imediata e encaminhado para a Departamento de Tecnologia da Informação para providências quanto ao cadastramento, habilitação e inabilitação, que será realizado nos termos descrito no procedimento do anexo I.

§ 1º. O login na rede e os demais recursos da tecnologia da informação, são de uso pessoal e intransferível, sendo que toda a e qualquer ação executada por meio de um determinado usuário, será de responsabilidade daquele a quem o login foi atribuído, cabendo-lhe, portanto, zelar pela confidencialidade de sua senha.

§ 2º. Ao perder o vínculo com a Prefeitura todos os acessos do usuário aos recursos da tecnologia da informação serão excluídos, suas contas de e-mails canceladas e seu conteúdo apagado.

§ 3º. Fica o Departamento de Recursos Humanos responsável por repassar à Departamento de Tecnologia da Informação, a qualquer tempo, as demissões/exonerações, do quadro de funcionários, nos termos do Anexo I (item 3.1), para que as providências acima sejam tomadas.

Art. 11. A mensageria é o serviço, por meio de softwares, que permite a rápida comunicação interna entre as equipes de cada Departamento Municipal bem como externa, seja com empresas terceirizadas prestadoras de serviço ou munícipes.

§ 1º. A Política de utilização de aplicativo de mensageria (whatsapp, telegram, entre outros) institucional está descrita no Anexo V, do presente decreto.

Art. 12. O Departamento Municipal que tenha interesse em utilizar os aplicativos de mensageria (whatsapp, telegram, entre outros) institucional deverá realizar abertura de chamado junto ao Departamento de Tecnologia da Informação, para que esta analise a viabilidade e, posteriormente, realize a configuração.

Art. 13. O uso de mensageria institucional sujeita-se as seguintes regras de boas práticas:

I — é vedado o uso institucional de mensageria para dirimir assuntos pessoais;

II — é vedada a utilização de número de telefone particular no sistema de mensageria institucional;

III — observar e respeitar todos os termos, políticas e demais normas de utilização de mensageria, sistemas ou funcionalidades de titularidade de terceiros que se faça necessário acessar ou utilizar para fins e/ou por ocasião do uso regular dos módulos de *software* não personalizado que integram a Prefeitura Municipal de Capela do Alto, conforme legislação vigente;

IV — não divulgar, publicar ou incorporar em relação a suas mensagens conteúdo que:

a) viole a legislação ou direitos de terceiros garantidos por contrato ou instrumentos afins;
b) seja falso, ambíguo, inexato, exagerado, incompleto ou desatualizado, de forma que possa induzir o destinatário a erro;
c) tenha caráter ofensivo ou que possa implicar em qualquer tipo de violência, ameaça, calúnia, injuria, difamação;
d) incite a pratica de atos discriminatórios, seja em razão de sexo, raça, religião, crenças, idade ou qualquer outra condição;
c) caracterize violação ou invasão da privacidade e/ou intimidade;

f) constitua violação de direitos de propriedade intelectual, pirataria de *software*, produtos e/ou serviços protegidos por direitos autorais ou afins;

g) veicule, incite ou estimule a pedofilia ou atos relacionados à prostituição ou similares, material pornográfico, obsceno ou contrário à ética das relações intersubjetivas e aos bons costumes;

h) seja caracterizado como spam;

i) incorpore *malwares*; e

j) inclua links que possam remeter para sites que possuam quaisquer dos conteúdos mencionados acima.

Parágrafo único. É de responsabilidade exclusiva do usuário do serviço de mensageria o modo de tratamento entre funcionários e munícipes, ficando a cargo do Departamento Municipal onde o servidor está locado a fiscalização.

Art. 14. Fica proibida a utilização de mídias removíveis nos aparelhos e equipamentos tecnológicos da Prefeitura Municipal de Capela do Alto.
§ 1º. A Política de não utilização de mídias removíveis (HD externo, pen drive, entre outros) está descrita no Anexo VI, do presente Decreto.

Art. 15. Fica instituída a Política de Privacidade para acesso as imagens das câmeras de segurança da Prefeitura, nos termos do Anexo VII, do presente decreto.
Parágrafo único. Os servidores que terão acesso as imagens das câmeras de segurança da Prefeitura deverão firmar Termo de Compromisso e Responsabilidade, nos termos do anexo VIII do presente Decreto.

Art. 16. Fica instituído o Procedimento para Desenvolvimento e Aquisição de Software em Conformidade com a LGPD, nos termos do Anexo IX do presente decreto.

Art. 17. 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. 18. O usuário identificado como causador de ações indevidas aos recursos da tecnologia da informação terá seu *login* imediatamente suspenso pelo Departamento de Tecnologia da Informação, dando-se expressa ciência ao chefe máximo do Departamento Municipal respectivo.

Art. 19. O descumprimento das disposições contidas neste decreto caracteriza descumprimento de dever funcional, indisciplina ou insubordinação, conforme o caso, a ser apurada em Sindicância Administrativa ou Processo Administrativo Disciplinar, garantido o direito de ampla defesa e contraditório
Parágrafo único. A critério do chefe máximo do Departamento, uma vez instaurado o processo administrativo disciplinar, o usuário poderá ter a suspensão cautelar da correspondente autorização de uso, mediante bloqueio dos recursos da tecnologia da informação.

Art. 20. Sem prejuízo da incidência de regras previstas em normas especificas, as disposições deste Decreto se aplicam, no que couber, à modalidade de trabalho realizado a distância.

Art. 21. Compete ao superior imediato do usuário comunicar quaisquer ações que comprometam a segurança, a integridade, o desempenho e a descaracterização de equipamentos e redes da Prefeitura.

Art. 22. Este Decreto entra em vigor na data de sua publicação, revogadas as disposições em contrário.

Prefeitura Municipal de Capela do Alto, em 14 de novembro de 2024.

PÉRICLES GONÇALVES
PREFEITO MUNICIPAL

Registrado nesta Secretaria e publicado no Diário Oficial Eletrônico do Município, e, por afixação nesta Prefeitura Municipal, data supra.

VALDIR APARECIDO DE MORIAS
SECRET. ADMINISTRATIVO

ANEXO I

Procedimento de Habilitação e Inabilitação de Acessos dos Servidores aos Módulos do Sistema de Gestão da Prefeitura Municipal de *Capela do Alto*

1. Objetivo

Este procedimento tem como objetivo estabelecer diretrizes para a habilitação e inabilitação de acessos dos servidores aos módulos do Sistema de Gestão da Prefeitura Municipal de Capela do Alto. Ele define as responsabilidades e os processos a serem seguidos para garantir a correta atribuição de acessos aos servidores recém-contratados, bem como a inabilitação imediata dos acessos dos servidores exonerados. Além disso, estabelece um processo para lidar com perda ou esquecimento de senhas.

2. Habilitação de Acessos

2.1. Encaminhamento de Dados do Servidor

A Secretaria de cada pasta é responsável por encaminhar ao Departamento de Tecnologia da Informação os dados do servidor recém-contratado, indicando quais módulos ele deve acessar. Essas informações devem ser fornecidas de forma clara e completa, incluindo o nome do servidor, setor de atuação e os serviços e módulos específicos que ele precisa acessar.

2.2. Cadastro e Habilitação

Com base nas informações recebidas, o Departamento de Tecnologia da Informação será responsável por cadastrar o novo servidor no Sistema de Gestão e habilitar os acessos aos módulos indicados. O Departamento de Tecnologia da Informação deve gerar um “login ou ID do usuário” e uma senha provisória que será enviada ao servidor para que ele possa acessar o sistema inicialmente.

§ 1° Ao usuário será fornecido o “login ou ID do usuário”, sobre o qual deverá tomar ciência e, assim, assinar o termo de responsabilidade de acesso aos recursos da tecnologia da informação, constante no Anexo II.

§ 2° Após o cadastro, o usuário deverá registrar/alterar sua senha, que será de uso pessoal e intransferível, sendo que as senhas cadastradas no SCPI8 e no Flowdocs devem ser iguais, a qual permitirá o seu login na rede de computadores da Prefeitura e aos recursos da tecnologia da informação.

§ 3° Qualquer mudança de lotação dos usuários deverá ser comunicada imediatamente pelo setor de origem, através da chefia imediata para que sejam realizados os ajustes necessários no seu cadastro.

§ 4° Qualquer mudança que venha a ocorrer do perfil do usuário, seja de alteração do perfil de acesso, ampliação ou exclusão de permissões deverá ser comunicado pela chefia imediata.

2.3. Alteração de Senha Provisória

É responsabilidade do servidor alterar a senha provisória assim que acessar o sistema pela primeira vez. Essa senha deve ser alterada para uma senha pessoal e segura de acordo com as políticas de segurança estabelecidas, registrando que as senhas cadastradas no SCPI8 e no Flowdocs devem ser iguais.

3. Inabilitação de Acessos

3.1. Exoneração do Servidor

O Departamento de Recursos Humanos (RH) deve encaminhar oficialmente ao Departamento de Tecnologia da Informação a informação da exoneração do servidor. Essa comunicação deve ser realizada imediatamente após a exoneração, incluindo o nome do servidor e a data da exoneração.

3.2. Inabilitação de Acesso

Com base nas informações fornecidas pelo Departamento de Recursos Humanos, o Departamento de Tecnologia da Informação será responsável por realizar a inabilitação do acesso do servidor exonerado. O acesso deve ser revogado de forma imediata para garantir a segurança dos dados e sistemas.

4. Perda ou Esquecimento de Senha

4.1. Solicitação de Nova Senha

Em caso de perda ou esquecimento da senha, o servidor deve encaminhar um e-mail ao Departamento de Tecnologia da Informação solicitando a geração de uma nova senha. O e-mail deve conter as informações necessárias para identificar o servidor, como o nome e cargo.

4.2. Geração de Nova Senha

O Departamento de Tecnologia da Informação será responsável por gerar uma nova senha para o servidor e encaminhá-la de forma segura. O servidor deverá ser orientado a alterar a senha novamente assim que fizer o login no sistema.

5. Responsabilidades

- Secretarias, Diretorias, Divisões: Responsáveis por encaminhar os dados do servidor recém-contratado e indicar quais módulos ele deve acessar.
- Departamento de Tecnologia da Informação: Responsável por cadastrar, habilitar e conceder acesso aos módulos do sistema aos servidores, bem como por inabilitar o acesso dos servidores exonerados e gerar novas senhas em caso de perda ou esquecimento.
- Recursos Humanos (RH): Responsável por comunicar oficialmente ao Departamento de Tecnologia da Informação a exoneração do servidor.

6. Revisão do Procedimento

Este procedimento será revisado periodicamente para garantir sua conformidade contínua com as necessidades e as melhores práticas da Prefeitura Municipal de Capela do Alto.

Este procedimento estabelece um fluxo claro e responsabilidades definidas para o cadastro, habilitação e inabilitação de acessos dos servidores aos módulos do Sistema de Gestão da Prefeitura Municipal de *Capela do Alto*.

Ao seguir essas diretrizes, garantimos a segurança e o controle adequados sobre os acessos aos sistemas, bem como o cumprimento das obrigações estabelecidas pela Lei Geral de Proteção de Dados (LGPD) e outras regulamentações aplicáveis.

ANEXO II

FICHA DE SOLICITAÇÃO DE CADASTRO / INCLUSÃO / EXCLUSÃO DE ACESSOS A SERVIÇOS DE TI

1 - INFORMAÇÕES GERAIS

UNIDADE/SETOR SOLICITANTE: _____ DATA: _____

NOME COMPLETO DO USUÁRIO: _____

Matrícula nº _____

SOLICITAÇÃO DE: ( ) INCLUSÃO/ALTERAÇÃO
( ) DESBLOQUEIO*

EXCLUSÃO* DE USUÁRIO POR MOTIVO DE:
( ) DESLIGAMENTO
( ) OUTRO:
_____

BLOQUEIO* POR MOTIVO DE:
( ) FÉRIAS
( ) MAU USO
( ) OUTRO:
_____

* Para esta opção, não é necessário preencher o item 2 deste formulário.

2 – SERVIÇOS DISPONÍVEIS (Preencher somente para solicitações de inclusão ou modificação e acessos. Este campo deverá ser preenchido pelo Chefe Imediato, o qual definirá quais serviços o usuário terá direito de acesso).

CONTA PARA ACESSO AOS COMPUTADORES DA REDE. .( ) PERMITIDO ( ) NÃO PERMITIDO
PERMISSÃO DE ACESSO À INTERNET ( ) PERMITIDO ( ) NÃO PERMITIDO
CORREIO ELETRÔNICO (E-MAIL) ( ) PERMITIDO ( ) NÃO PERMITIDO
SISTEMAS DE INFORMAÇÃO ( ) PERMITIDO ( ) NÃO PERMITIDO

2.1 – MÓDULOS AUTORIZADOS (Preencher somente para solicitações de inclusão ou modificação e acessos. Este campo deverá ser preenchido pelo Chefe Imediato, o qual definirá quais módulos o usuário terá direito de acesso).

MÓDULO ..... ( ) PERMITIDO ( ) NÃO PERMITIDO
MÓDULO ..... ( ) PERMITIDO ( ) NÃO PERMITIDO
MÓDULO ..... ( ) PERMITIDO ( ) NÃO PERMITIDO
MÓDULO ..... ( ) PERMITIDO ( ) NÃO PERMITIDO
MÓDULO ..... ( ) PERMITIDO ( ) NÃO PERMITIDO
MÓDULO ..... ( ) PERMITIDO ( ) NÃO PERMITIDO
MÓDULO ..... ( ) PERMITIDO ( ) NÃO PERMITIDO
MÓDULO ..... ( ) PERMITIDO ( ) NÃO PERMITIDO

MÓDULO .... ( ) PERMITIDO ( ) NÃO PERMITIDO
MÓDULO .... ( ) PERMITIDO ( ) NÃO PERMITIDO
MÓDULO .... ( ) PERMITIDO ( ) NÃO PERMITIDO
MÓDULO .... ( ) PERMITIDO ( ) NÃO PERMITIDO
MÓDULO .... ( ) PERMITIDO ( ) NÃO PERMITIDO
MÓDULO .... ( ) PERMITIDO ( ) NÃO PERMITIDO
MÓDULO .... ( ) PERMITIDO ( ) NÃO PERMITIDO
MÓDULO .... ( ) PERMITIDO ( ) NÃO PERMITIDO
MÓDULO .... ( ) PERMITIDO ( ) NÃO PERMITIDO
MÓDULO .... ( ) PERMITIDO ( ) NÃO PERMITIDO
MÓDULO .... ( ) PERMITIDO ( ) NÃO PERMITIDO
MÓDULO .... ( ) PERMITIDO ( ) NÃO PERMITIDO
MÓDULO .... ( ) PERMITIDO ( ) NÃO PERMITIDO

3 - AUTORIZAÇÃO

ASSINATURA DO USUÁRIO

____

Assinando o presente, o usuário aceita todas as normas estabelecidas pela Prefeitura Municipal de Capela do Alto

ASSINATURA DO CHEFE IMEDIATO PELA UNIDADE

____

Nome completo do Chefe Imediato e Matrícula:

____

4 – CAMPOS A SEREM PREENCHIDOS PELO DEPARTAMENTO DE TECNOLOGIA DA INFORMAÇÃO

Data do Recebimento: _____________________ Data do Atendimento: _____________________

Assinatura do Responsável:

____

ANEXO III

TERMO DE RESPONSABILIDADE
ACESSO AOS RECURSOS TECNOLOGIA DA INFORMAÇÃO

Eu, _____, declaro haver solicitado acesso aos Recursos da Tecnologia da Informação e comprometo-me a:

1. Acessar a internet/intranet somente por necessidade de serviço ou por determinação expressa de superior hierárquico, realizando as tarefas e operações em estrita observância aos procedimentos, normas e disposições contidas no decreto que rege o acesso à internet/intranet e utilização de *e-mails*;

2. Utilizar a caixa postal (*e-mail*) colocada a minha disposição somente por necessidade de serviço ou por determinação expressa de superior hierárquico, realizando as tarefas e operações, em estrita observância aos procedimentos, às normas e às disposições contidas na instrução normativa que rege o acesso à internet/intranet e utilização de *e-mails*;

3. Não revelar, fora do âmbito profissional, fatos, dados ou informação de qualquer natureza de que tenha conhecimento por força de minhas atribuições, salvo em decorrência de decisão competente na esfera legal ou judicial, bem como de autoridade superior;

4. Manter a necessária cautela quando da exibição de dados em tela, impressora ou na gravação em meios eletrônicos, a fim de evitar que deles venham a tomar ciência pessoas não autorizadas;

5. Não me ausentar da estação de trabalho sem encerrar a sessão de uso do navegador (*browser*), garantindo, assim, a impossibilidade de acesso indevido por terceiros;

6. Não revelar minha senha de acesso à internet/intranet e de minha caixa postal (*e-mail)* a ninguém e tomar o máximo de cuidado para que ela permaneça somente de meu conhecimento;

7. Responder, em todas as instâncias, pelas consequências das ações ou omissões de minha parte que possam pôr em risco ou comprometer a exclusividade de conhecimento de minha senha ou das transações a que tenha acesso.

8. Declaro, ainda, estar plenamente esclarecido e consciente das cláusulas que regem o Decreto 3.754/2024, enfatizando, entre outras, que:

8.1. Não é permitida a navegação em *sites* pornográficos, defensores do uso de drogas, de pedofilia ou *sites* de cunho racista e similares;

8.2. É de minha responsabilidade cuidar da integridade, confidencialidade e disponibilidade das informações contidas em minha caixa postal (*e-mail*), devendo comunicar por escrito à chefia imediata quaisquer indícios ou possibilidades de irregularidades, de desvios ou falhas identificadas no sistema de correio, sendo proibida a exploração de falhas ou vulnerabilidades porventura existentes;

8.3. O acesso à informação de minha caixa postal (*e-mail*) não me garante direito sobre ela, uma vez que faço uso para melhor desempenhar minhas atividades administrativas, nem me confere autoridade para liberar acesso a outras pessoas, pois se constitui de informações pertencentes à Administração Municipal;

8.4. Constitui descumprimento de normas legais, regulamentares e quebra de sigilo funcional divulgar dados obtidos por meio do uso de minha caixa postal (*e-mail*), a qual tenho acesso,

para outros servidores não envolvidos nos trabalhos executados;

8.5. Devo alterar minha senha, sempre que obrigatório ou que tenha suspeição de descoberta por terceiros, não usando combinações simples que possam ser facilmente descobertas;

8.6. Respeitar as normas de segurança e restrições de sistema impostas pelos sistemas de segurança implantados na instituição;

8.7. Cumprir e fazer cumprir os dispositivos da Política de Segurança da Informação, de suas diretrizes, bem como deste Termo de Responsabilidade.

9. Ressalvadas as hipóteses de requisições legalmente autorizadas, constitui infração funcional a revelação de segredo do qual me apropriei em razão do cargo, sendo crime contra a Administração Pública a divulgação a quem não seja servidor da Prefeitura, das informações ou dados a(s) qual(is) tenho acesso, estando sujeito às penalidades previstas em lei;

10. Sem prejuízo da responsabilidade penal e civil, e de outras infrações disciplinares, constitui falta de zelo e dedicação às atribuições do cargo e descumprimento de normas legais e regulamentares não proceder com cuidado na guarda e utilização de senha ou emprestá-la a outro servidor, ainda que habilitado;

11. Constitui infração funcional e penal enviar ou facilitar o envio por terceiros de *e-mails* falsos, ficando o infrator sujeito à punição com a demissão, conforme responsabilização por crime contra a Administração Pública, tipificado nos artigos 313-A e 313-B, do Código Penal Brasileiro (Decreto-Lei nº 2.848, de 1940).

Declaro, nesta data, ter ciência e estar de acordo com os procedimentos anteriormente descritos, comprometendo-me a respeitá-los e cumpri-los plena e integralmente. USUÁRIO. Capela do Alto, ____de _____ de_____ **Assinatura**_____	**RESERVADO PARA O DTI** **Assinatura:**

ANEXO IV
POLÍTICA DE BACKUP E RESTAURAÇÃO DE DADOS

INTRODUÇÃO

A Política de Backup e Restauração de Dados objetiva instituir diretrizes, responsabilidades e competências que visam à segurança, proteção e disponibilidade dos dados custodiados pelo Departamento de Tecnologia da Informação (DTI) para manter a continuidade das atividades institucionais da Prefeitura do Município de Capela do Alto.
A implantação desta política busca assegurar sua missão, sendo necessário estabelecer mecanismos que permitam a guarda de dados e sua eventual restauração em casos de indisponibilidade ou perda por erro humano, ataques cibernéticos ou outras ameaças. Busca estabelecer o modo e a periodicidade da cópia de dados armazenados pelos sistemas computacionais.
Considera-se como "dados críticos" pastas armazenadas no servidor de dados, banco de dados dos sistemas de informações corporativas, de folha de pagamento, tramitação de documentos e e-mails devendo ser revisado anualmente a definição de dados críticos e o escopo desta política de backup.
Esta política se aplica aos servidores da DTI que armazenam tais dados. A política também se aplica a terceiros que processam e armazenam dados de propriedade da Prefeitura.

CONCEITOS

Backup ou Cópia de Segurança: conjunto de procedimentos que permitem salvaguardar os dados de um sistema computacional, garantindo a guarda, proteção e recuperação Têm a fidelidade ao original assegurada.
Deve ser identificado a mídia em que a cópia é realizada;
Custodiante da Informação: qualquer indivíduo ou estrutura da Prefeitura que tenha a responsabilidade formal de proteger a informação e aplicar os níveis de controle de segurança em conformidade com as exigências de Segurança da Informação comunicadas pelo proprietário da informação;
Eliminação: exclusão de dados ou conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado;
Mídia: mecanismos em que os dados podem ser armazenados;
Infraestrutura Crítica: Instalações, serviços, bens e sistemas, virtuais ou físicos, que se forem incapacitados ou tiverem desempenho degradado, provocarão forte impacto na rotina de trabalho da Prefeitura;
Recovery Point Objective (RPO): ponto no tempo em que os dados dos serviços de TI devem ser recuperados após uma situação de parada ou perda, correspondendo ao prazo máximo em que se admite perder dados no caso de um incidente;
Recovery Time Objective (RTO): tempo estimado para restaurar os dados e tornar os serviços de TI novamente operacionais, correspondendo ao prazo máximo em que se admite manter os serviços de TI inoperantes até a restauração de seus dados, após um incidente.

PRINCÍPIOS GERAIS

A Política de Backup e Restauração de Dados deve estar alinhada com a Política de Segurança da Informação, bem como com a gestão de continuidade das atividades.
As rotinas de backup devem ser orientadas para a restauração dos dados no menor tempo possível, principalmente quando da indisponibilidade de serviços de TI.
As rotinas de backup devem utilizar soluções próprias e especializadas para este fim, preferencialmente de forma automatizada.
As rotinas de backup devem possuir requisitos mínimos diferenciados de acordo com o tipo de serviço de TI ou dado armazenado, dando prioridade aos serviços de TI críticos da Prefeitura.
O armazenamento de backup, se possível, deve ser realizado em um local distinto da infraestrutura crítica.

A infraestrutura de rede de backup deve ser separada dos sistemas críticos da Prefeitura. Nos casos em que a confidencialidade for importante, convém que as cópias de segurança sejam protegidas através de criptografia apropriada.
Os backups críticos devem ser realizados diariamente.
Os serviços críticos de TI, armazenados em nuvem, devem ser resguardados sob um padrão de segurança, devendo observar a frequência da retenção de dados estabelecida abaixo:
Diária: 1 mês;
Mensal: 1 ano;
Anual: 5 anos.
Os serviços não críticos de TI, armazenados em nuvem ou infraestrutura local, devem ser resguardados sob um padrão de segurança, devendo observar a frequência da retenção de dados estabelecidas abaixo:
Diária: 1 mês;
Mensal: 1 ano;
Anual: 1 ano.
Especificações dos serviços de TI críticos e dos serviços de TI não críticos podem demandar frequência e tempo de retenção diferenciados.
Os ativos envolvidos no processo de backup são considerados ativos críticos para a organização.
A alteração das frequências e tempos de retenção definidos nesta seção será precedida de solicitação e justificativa formais encaminhadas à DTI para análise e aprovação.
Os responsáveis pelos dados deverão ter ciência dos tempos de retenção estabelecidos para cada tipo de informação e os administradores de backup deverão zelar pelo cumprimento das regras estabelecidas.

TIPOS DE BACKUP
Para fins de realização de backup serão utilizados os seguintes modelos:
- Completo (Full);
- Incremental.

Salvo indicação em contrário, o backup dos dados do sistema será feito de acordo com a programação padrão:
- Backup incremental diário;
- Backup completo semanal.

Os backups serão armazenados na infraestrutura de rede de backup. Os backups deverão ser realizados no período noturno para permitir mais tempo para realizar o backup e o baixo processamento dos servidores de dados.

IMPACTOS E ARMAZENAMENTO
Deve ser considerado o impacto da execução das rotinas de backup sobre o desempenho da rede de dados da Prefeitura, garantindo que o tráfego necessário às suas atividades não ocasione indisponibilidade dos demais serviços de TI da instituição.

As unidades de armazenamento utilizadas no armazenamento dos dados devem considerar as características de cada dado armazenado, tais como:
- A criticidade do dado armazenado;
- O tempo necessário de retenção do dado;
- A probabilidade de necessidade de restauração;
- O tempo previsto de restauração;
- O custo de aquisição e manutenção da unidade de armazenamento de backup;
- A vida útil da unidade de armazenamento de backup.

O Departamento de Tecnologia da Informação deve identificar a viabilidade de utilização de diferentes tecnologias na realização das cópias de segurança, propondo a melhor solução para cada caso.

A execução das rotinas de backup deve considerar a previsão de ampliação da capacidade dos dispositivos envolvidos para o armazenamento local e em nuvem.
As unidades de armazenamento de backup devem estar instaladas em locais apropriados, com controle de temperatura, umidade, poeira e de acesso restrito a pessoas de acordo com as normas técnicas que tratam de segurança física e lógica destes equipamentos.
Quando ocorrer a necessidade de descarte de unidades de armazenamento de backups, tais recursos devem ser fisicamente destruídos, de forma a inutilizá-los, atentando-se ao descarte sustentável conforme normas ambientais para equipamentos de TI.

VALIDAÇÃO
Diariamente, deverão ser revisados os logs em busca de erros, durações anormais e quando possível a oportunidade para melhoria do desempenho do backup;
Ações corretivas serão tomadas quando forem identificados os problemas de backup, a fim de reduzir os riscos associados a falhas de backup;
Deverá ser mantido registro de backups e de testes de restauração para demonstrar a conformidade com esta política.
Os testes de restauração de backups devem ser realizados por amostragem, uma vez por mês, em equipamentos servidores diferentes dos equipamentos que atendem os ambientes de produção, a fim de verificar backups bem-sucedidos.
Será necessário verificar se foram atendidos os níveis de serviço de Recovery Time Objective - RTOs.
Os registros deverão conter, no mínimo, o tipo de sistema que teve seu restabelecimento testado, a data da realização do teste, o tempo gasto para o retorno de backup e se o procedimento foi realizado com sucesso.

RESTAURAÇÃO
O atendimento de solicitações de restauração de backup de arquivos, banco de dados e demais formas de dado deverá obedecer aos seguintes procedimentos:
- A solicitação de restauração deverá sempre partir do responsável pelo dado, através de chamado técnico;
- A restauração somente será possível nos casos em que este tenha sido atingido pela estratégia de backup;
- A restauração poderá ser negada nos casos cujo conteúdo não seja condizente com a atividade da área solicitante, cabendo recurso da negativa solicitado pelo secretário da pasta solicitante com as justificativas da solicitação;
- O tempo de restauração é proporcional ao volume de dados necessários para o restore de dados, devendo ser estabelecido por meio de acordo de nível de serviço o tempo para atendimento estas solicitações.

DESCARTES
Nos casos de desligamento do usuário (de forma permanente ou temporária), o backup de seus arquivos respeitará as diretrizes de política de descarte. Após o período determinado, os arquivos poderão ser excluídos a qualquer momento.
A mídia de backup será retirada e descartada conforme descrito nesta política de backup;
Deverá ser garantido que a mídia não contenha mais imagens de backup ativas e que o conteúdo atual ou anterior não possa ser lido ou recuperado por terceiros não autorizados.

O Departamento de Tecnologia da Informação deverá garantir a destruição física da mídia antes do descarte.

CONSIDERAÇÕES FINAIS
Dados armazenados localmente por usuários fora do conhecimento da DTI não estão cobertos por esta política. É responsabilidade do usuário/departamento a gestão desses dispositivos e dados.

ANEXO V

POLÍTICA DE UTILIZAÇÃO DE APLICATIVO DE MENSAGERIA (WHATSAPP, TELEGRAM, ENTRE OUTROS) INSTITUCIONAL PARA ATENDIMENTO AO CIDADÃO DA PREFEITURA MUNICIPAL

1. Objetivo

Esta política tem como objetivo estabelecer diretrizes para o uso de aplicativo de mensageria (whatsapp, telegram, entre outros) institucional como canal de comunicação para atendimento aos cidadãos pela Prefeitura Municipal de Capela do Alto, com foco na proteção de dados pessoais e no cumprimento da Lei Geral de Proteção de Dados (LGPD).

2. Uso Autorizado de Aplicativo de Mensageria (whatsapp, telegram, entre outros) Institucional

2.1. O aplicativo de mensageria (whatsapp, telegram, entre outros) institucional será utilizado exclusivamente para o atendimento aos cidadãos, esclarecimento de dúvidas, prestação de informações e serviços relacionados às atividades da Prefeitura Municipal de Capela do Alto.

2.2. Os funcionários designados para o atendimento via aplicativo de mensageria (whatsapp, telegram, entre outros) institucional devem seguir as orientações estabelecidas nesta política.

2.3. É estritamente proibida a utilização de aplicativo de mensageria pessoal para fins de atendimento e coleta de dados em nome da Prefeitura.

3. Coleta de Dados

3.1. Durante o atendimento, podem ser coletados dados pessoais dos cidadãos, como nome, número de telefone, email, bem como outros dados e informações relacionadas aos serviços solicitados.

3.2. Os funcionários responsáveis pelo atendimento devem garantir que apenas informações estritamente necessárias ao atendimento sejam coletadas e que o consentimento do cidadão não seja necessário, uma vez que os dados serão eliminados imediatamente após o atendimento.

4. Eliminação Imediata de Dados

4.1. Após o término do atendimento ou a conclusão do propósito, os dados pessoais coletados via aplicativo de mensageria (whatsapp, telegram, entre outros) institucional devem ser prontamente eliminados, de forma irreversível.

4.2. É proibido o armazenamento ou registro de dados pessoais dos cidadãos em qualquer meio ou dispositivo após a conclusão do atendimento.

5. Segurança dos Dados

5.1. A Prefeitura deve adotar medidas de segurança adequadas para proteger os dados pessoais coletados, mesmo que temporariamente, durante o atendimento.

6. Treinamento dos Funcionários

6.1. Todos os funcionários que realizam atendimento via aplicativo de mensageria (whatsapp, telegram, entre outros) institucional devem ser treinados em relação às diretrizes desta política e às obrigações da LGPD.

7. Revisão da Política

7.1. Esta política será revisada periodicamente para garantir a conformidade com as leis e regulamentos aplicáveis.

8. Penalidades

8.1. O não cumprimento desta política e das regulamentações de privacidade pode resultar em sanções, de acordo com a LGPD e demais leis aplicáveis.

Esta política de utilização de aplicativo de mensageria (whatsapp, telegram, entre outros) institucional deve ser divulgada e comunicada a todos os funcionários responsáveis pelo atendimento, e é importante manter registros documentados das eliminações de dados para fins de comprovação de conformidade com a LGPD.

ANEXO VI

POLÍTICA DE NÃO UTILIZAÇÃO DE MÍDIAS REMOVÍVEIS (HD EXTERNO E PEN DRIVE)

1. Objetivo

Esta política estabelece diretrizes para a não utilização de dispositivos de armazenamento externo, como HDs externos e pen drives, e a substituição desses dispositivos por soluções baseadas em nuvem, visando garantir a segurança e a integridade dos dados da Prefeitura Municipal de Capela do Alto.

2. Justificativa

A utilização de mídias removíveis (HDs externos e pen drives) apresenta riscos à segurança e proteção dos dados, como perda, roubo, danos físicos, malware e compartilhamento não autorizado de informações confidenciais. A adoção de soluções de armazenamento em nuvem oferece maior segurança, acessibilidade e colaboração, além de possibilitar o backup regular e a recuperação de dados em casos de incidentes.

3. Diretrizes

3.1. Proibição do Uso de mídias removíveis (HD Externo e Pen Drive)

Fica proibido o uso de mídias removíveis como meio de armazenamento e transferência de dados por parte dos servidores da Prefeitura Municipal de Capela do Alto, exceto em casos excepcionais devidamente autorizados pela área responsável.

3.2. Utilização de Soluções de Armazenamento em Nuvem

Recomenda-se que os servidores utilizem soluções de armazenamento em nuvem aprovadas pela Prefeitura Municipal de Capela do Alto para armazenar, compartilhar e transferir documentos e dados. Essas soluções devem ser seguras, confiáveis e compatíveis com as políticas de segurança de informações da Prefeitura Municipal de Capela do Alto.

3.3. Backup Regular e Segurança dos Dados na Nuvem

Os servidores devem realizar backups regulares de seus dados armazenados em soluções em nuvem, de acordo com as diretrizes e procedimentos estabelecidos pela Prefeitura Municipal de Capela do Alto. É responsabilidade dos servidores garantir a segurança de suas contas e senhas, bem como utilizar mecanismos de autenticação em dois fatores quando disponíveis.

3.4. Conscientização e Treinamento

A Prefeitura Municipal de Capela do Alto promoverá treinamentos e ações de conscientização periódicas para informar os servidores sobre a importância da não utilização de mídias removíveis, assim como para instruí-los sobre o uso correto das soluções de armazenamento em nuvem.

4. Responsabilidades

4.1. Área de Tecnologia da Informação (T.I.)

A área de T.I. será responsável por:

a) Identificar e implementar soluções de armazenamento em nuvem seguras e adequadas às necessidades da instituição;

b) Monitorar o cumprimento desta política e realizar auditorias periódicas;

c) Fornecer suporte técnico e orientações aos servidores sobre o uso das soluções em nuvem aprovadas.

4.2. Servidores

Os servidores da Prefeitura Municipal de Capela do Alto devem:

a) Abster-se de utilizar mídias removíveis como forma de armazenamento e transferência de dados;

b) Utilizar as soluções de armazenamento em nuvem aprovadas pela instituição para armazenar e compartilhar documentos e dados;

c) Realizar backups regulares dos dados armazenados na nuvem;

d) Manter suas contas e senhas de acesso seguras e protegidas.

5. Revisão da Política

Esta política será revisada periodicamente para garantir sua conformidade contínua com as necessidades e melhores práticas da Prefeitura Municipal de Capela do Alto, bem como em conformidade com a legislação vigente.

Esta política visa garantir a segurança e a integridade dos dados da Prefeitura Municipal de Capela do Alto, protegendo-os contra riscos associados à utilização de mídias removíveis.

Ao adotar soluções de armazenamento em nuvem e seguir as diretrizes estabelecidas nesta política, a Prefeitura Municipal de Capela do Alto busca promover uma cultura de segurança da informação e proteção dos dados.

ANEXO VII
POLÍTICA DE PRIVACIDADE – ACESSO A IMAGENS DE CÂMERAS DE SEGURANÇA DA PREFEITURA MUNICIPAL DE CAPELA DO ALTO

Esta Política de Privacidade tem como objetivo estabelecer diretrizes para o acesso e tratamento de imagens captadas por câmeras de segurança instaladas nos órgãos públicos municipais, em conformidade com a Lei Geral de Proteção de Dados (LGPD) [Lei nº 13.709/2018].

Nesta política, fica estabelecido que o acesso às imagens será restrito a determinados cargos e funções, garantindo a privacidade e a proteção dos dados pessoais.

1. Acesso Restrito às Imagens de Câmeras de Segurança:

1.1. O acesso às imagens de câmeras de segurança será permitido somente aos seguintes cargos e funções, desde que seja necessário para o cumprimento das suas atribuições funcionais:

a) Chefe do Departamento onde a câmera de segurança estiver instalada;
b) Secretário ou Diretor de Departamento;
c) Responsável pela segurança do órgão público;
d) Chefe do Departamento de Tecnologia da Informação;
e) Guarda Civil Municipal.

1.2. Todos os servidores mencionados acima que tenham acesso às imagens de câmeras de segurança devem passar por treinamentos e capacitações específicas sobre a proteção de dados pessoais e a importância de garantir a privacidade dos indivíduos captados pelas câmeras.

2. Uso Adequado das Imagens:

2.1. O acesso às imagens de câmeras de segurança deve ser utilizado exclusivamente para fins institucionais e no cumprimento das atribuições dos cargos mencionados.

2.2. É expressamente proibido o uso das imagens para obter informações pessoais de servidores, munícipes ou terceiros, ou para qualquer finalidade que viole a privacidade e os direitos fundamentais das pessoas.

3. Compartilhamento de Imagens:

3.1. As imagens captadas pelas câmeras de segurança não devem ser compartilhadas com servidores que não pertençam aos cargos autorizados descritos no item 1.1 desta política, exceto em situações estritamente necessárias para cumprir obrigações legais ou a pedido de autoridades policiais ou judiciárias.

3.2. O compartilhamento das imagens com terceiros ou fora do âmbito institucional deve ser realizado somente mediante consentimento expresso dos indivíduos captados pelas câmeras ou mediante uma das hipóteses legais descritas nos artigos 7º e 11 da Lei Geral de Proteção de Dados.

4. Armazenamento e Prazo de Retenção:

4.1. As imagens captadas pelas câmeras de segurança devem ser armazenadas em ambiente seguro e com acesso restrito aos cargos autorizados mencionados no item 1.1.

4.2. O prazo de retenção das imagens será estabelecido de acordo com a legislação aplicável e a política interna do órgão público, respeitando-se o tempo necessário para cumprir as finalidades legítimas da coleta.

5. Responsabilidade e Comunicação de Incidentes:

5.1. Os servidores com acesso às imagens de câmeras de segurança são responsáveis por garantir a segurança, integridade e privacidade dos dados pessoais.

5.2. Em caso de incidentes de segurança, acesso não autorizado ou suspeita de violação das imagens captadas pelas câmeras, o ocorrido deve ser comunicado imediatamente ao Encarregado de Proteção de Dados da Prefeitura Municipal.

6. Alterações na Política de Privacidade:

6.1. Esta Política de Privacidade poderá ser atualizada periodicamente para refletir alterações nos procedimentos de tratamento de dados ou atualizações na legislação vigente.

ANEXO VIII

TERMO DE COMPROMISSO DE ACESSO À IMAGENS DE CÂMERAS DE SEGURANÇA DA PREFEITURA MUNICIPAL DE CAPELA DO ALTO

Eu, [NOME DO SERVIDOR], portador da matrícula funcional nº [NÚMERO DA MATRÍCULA], servidor público da Prefeitura Municipal de Capela do Alto, declaro estar ciente e concordo plenamente com as responsabilidades e obrigações relacionadas ao acesso e tratamento de imagens captadas por câmeras de segurança instaladas nas dependências municipais sob minha responsabilidade.

2. Deveres e Responsabilidades:

1.1. Comprometo-me a utilizar o acesso às imagens de câmeras de segurança exclusivamente para o cumprimento das minhas atribuições e obrigações funcionais, relacionadas à segurança, proteção do patrimônio público e preservação da ordem.

1.2. Declaro que as imagens captadas pelas câmeras de segurança podem conter informações sensíveis e confidenciais, e me comprometo a mantê-las em absoluto sigilo, não as divulgando a terceiros ou utilizando-as para fins pessoais ou alheios ao interesse público.

1.3. Entendo que o acesso às imagens de câmeras de segurança é restrito e intransferível, sendo expressamente proibido compartilhar minha senha ou fornecer acesso a qualquer pessoa não autorizada.

1.4. Comprometo-me a adotar as medidas de segurança necessárias para evitar acesso não autorizado a dispositivos ou sistemas que contenham as imagens das câmeras de segurança.

2. Utilização Adequada:

2.1. As imagens captadas pelas câmeras de segurança são destinadas exclusivamente para fins institucionais, sendo estritamente proibida a utilização das mesmas para qualquer finalidade que não esteja alinhada com as atribuições do meu cargo.

2.2. Em hipótese alguma, utilizarei as imagens para obter informações pessoais de servidores, munícipes ou terceiros, ou para qualquer fim que possa violar a privacidade e os direitos fundamentais das pessoas.

2.3. Caso seja necessário utilizar as imagens em procedimentos administrativos ou judiciais, garantirei que a solicitação e divulgação sejam feitas de acordo com a legislação vigente, assegurando a privacidade e os direitos dos indivíduos envolvidos.

3. Comunicação de Incidentes:

3.1. Comprometo-me a notificar imediatamente meus superiores e o Encarregado de Proteção de Dados da Prefeitura Municipal de Capela do Alto sobre qualquer incidente de segurança, acesso não autorizado ou suspeita de violação das imagens captadas pelas câmeras.

4. Treinamento e Capacitação:

4.1. Estou ciente da importância de participar de treinamentos e capacitações oferecidos pela da Prefeitura Municipal de Capela do Alto referentes à segurança de dados, privacidade e à utilização adequada das imagens de câmeras de segurança.

5. Responsabilidades em Caso de Descumprimento:

5.1. Estou ciente de que o descumprimento das obrigações e responsabilidades estabelecidas neste termo poderá acarretar em medidas disciplinares, administrativas e legais, conforme a legislação aplicável.

6. Validade do Termo:

6.1. Este termo de compromisso entra em vigor a partir da data de sua assinatura e terá validade enquanto perdurar meu vínculo funcional com a da Prefeitura Municipal de Capela do Alto ou até que haja a revogação do acesso às imagens de câmeras de segurança.

Ao assinar este documento, declaro estar ciente e concordar integralmente com os termos da Política de Privacidade relativo ao acesso as imagens de câmeras de segurança, comprometendo-se a cumprir rigorosamente suas diretrizes.

Declaro, por fim, que li e compreendi integralmente o teor deste termo e assumo o compromisso de cumpri-lo fielmente, zelando pela segurança, privacidade e uso adequado das imagens captadas pelas câmeras de segurança.

Capela do Alto, [DATA]

Assinatura do Servidor: _____
(Nome do Servidor)

Testemunha 1: _____
(Nome e Assinatura)

Testemunha 2: _____
(Nome e Assinatura)

ANEXO IX
PROCEDIMENTO PARA DESENVOLVIMENTO E AQUISIÇÃO DE SOFTWARE EM CONFORMIDDE COM A LGPD

1. Objetivo

Este procedimento estabelece diretrizes para o desenvolvimento e aquisição de software pela Prefeitura Municipal de Capela do Alto, de acordo com as exigências da Lei Geral de Proteção de Dados (LGPD). O objetivo é garantir a privacidade e a segurança dos dados pessoais tratados nos sistemas utilizados pela Prefeitura Municipal de Capela do Alto.

2. Levantamento de Requisitos

2.1. Coleta de Dados Pessoais

Ao realizar o levantamento de requisitos para o desenvolvimento ou aquisição de software, é necessário identificar quais dados pessoais serão coletados, processados e armazenados nos sistemas. Essa análise deve considerar os princípios da minimização de dados, finalidade específica e necessidade de consentimento, quando aplicável.

2.2. Análise de Riscos e Medidas de Segurança

Deve ser realizada uma análise de riscos para identificar eventuais vulnerabilidades que possam comprometer a segurança dos dados pessoais. Com base nessa análise, medidas de segurança adequadas devem ser definidas e implementadas para mitigar esses riscos.

3. Desenvolvimento de Software

3.1. Princípios de Privacidade por Design

Durante o processo de desenvolvimento de software, os princípios de Privacidade por Design devem ser aplicados. Isso significa que a privacidade e a proteção de dados devem ser consideradas desde o início, com a implementação de medidas técnicas e organizacionais que garantam a conformidade com a LGPD.

3.2. Consentimento e Transparência

Quando o software envolver a coleta e o processamento de dados pessoais, é necessário que as políticas de privacidade e os termos de uso sejam transparentes, claros e facilmente acessíveis aos usuários. Além disso, sempre que a LGPD exigir, deve ser obtido o consentimento dos usuários de acordo com as diretrizes estabelecidas na Lei.

3.3. Minimização e Retenção de Dados

Os dados pessoais coletados devem ser limitados ao mínimo necessário para a finalidade específica do software. Além disso, os prazos de retenção de dados devem ser estabelecidos de acordo com a legislação aplicável e a política de retenção de dados da Prefeitura Municipal de Capela do Alto.

3.4. Segurança e Proteção de Dados

Medidas de segurança apropriadas devem ser implementadas para garantir a confidencialidade, integridade e disponibilidade dos dados pessoais. Isso inclui a utilização de criptografia, controle de acesso, monitoramento, backups regulares e outras medidas de proteção de dados.

4. Aquisição de Software

4.1. Avaliação de Fornecedores

Ao adquirir software de terceiros, é importante realizar uma avaliação criteriosa dos fornecedores, levando em consideração sua conformidade com a LGPD, medidas de segurança adotadas, política de privacidade, histórico e reputação.

4.2. Cláusulas Contratuais

Os contratos de aquisição de software devem incluir cláusulas específicas que garantam a conformidade com a LGPD e estabeleçam as responsabilidades das partes envolvidas em relação à proteção de dados pessoais.

5. Responsabilidades

- Departamento de Tecnologia da Informação: Responsável por garantir a conformidade com a LGPD nos processos de desenvolvimento e aquisição de software, implementando medidas de segurança e privacidade adequadas.

- Departamento Jurídico: Responsável por revisar contratos e orientar sobre as exigências legais da LGPD.

- Equipe de Desenvolvimento de Software: Responsável por aplicar os princípios de Privacidade por Design e desenvolver sistemas em conformidade com a LGPD.

6. Revisão do Procedimento

Este procedimento será revisado periodicamente para garantir sua conformidade contínua com as exigências da LGPD, bem como com as melhores práticas de proteção de dados pessoais.

Este procedimento tem como objetivo garantir que o desenvolvimento e aquisição de software pela Prefeitura Municipal de Capela do Alto estejam em conformidade com a LGPD.

Ao seguir essas diretrizes, buscamos proteger a privacidade e segurança dos dados pessoais tratados nos sistemas da instituição, garantindo o respeito aos direitos dos indivíduos em relação à proteção de seus dados pessoais.