PROJETO DE RESOLUÇÃO N° 000/2022

Estabelece boas práticas para proteção da informação, gestão de segurança e prevenção de incidentes relacionados a ativos de tecnologia da informação na câmara de Dilermando de Aguiar.

CAPÍTULO I
DISPOSIÇÕES PRELIMINARES

Art. 1º A Política de Segurança da Informação na Câmara de Vereadores de Dilermando de Aguiar aplica-se a todos os Vereadores, Servidores, prestadores de serviços, sistemas e serviços, incluindo trabalhos executados por terceiros que utilizem a infraestrutura da Casa ou acesso a informações eletrônicas pertencentes à Câmara de Vereadores de Dilermando de Aguiar.

Parágrafo único. Todo e qualquer usuário que tem acesso aos recursos tecnológicos disponibilizados pelo Setor de Informática tem a responsabilidade de zelar pela segurança e integridade das informações e dos equipamentos.

Art. 2º Esta política tem como objetivo aumentar o nível de segurança dos usuários e das informações, o método como os dados são acessados e estabelecer regras que contemplem as melhores práticas que podem ser aplicadas à Casa.

Art. 3º O Setor de Informática fica encarregado de conceder ou restringir acessos e senhas necessários para as tarefas de cada usuário dos recursos tecnológicos.

CAPÍTULO II
DA ADMISSÃO E EXONERAÇÃO DE SERVIDORES, TEMPORÁRIOS E ESTAGIÁRIOS

Art. 4º É necessária a comunicação ao Setor de Informática sobre todas as movimentações dos Servidores / temporários / externos) dentro da Casa, desde que esses possuam acesso a qualquer ativo de informática tais como computadores, sistemas, softwares de apoio, contas de e-mail e logins.

Art. 5º Compete ao setor de Recursos Humanos informar o Setor de Informática, no prazo de até 3 (três) dias úteis, a exoneração, o desligamento, mudança de setor ou mudança de atribuições que possuam acesso a qualquer ativo de informática para o posterior bloqueio ou ajuste de seu tipo de acesso.

CAPÍTULO III
DAS SENHAS E PERMISSÕES DE ACESSOS

Art. 6º Todo usuário poderá ter seu próprio login e senha, fornecidos pelo Setor de Informática, para executar suas funções dentro da rede informatizada da Câmara de Vereadores, bem como, para acesso aos sistemas, ficando obrigado a zelar pelo sigilo destas informações, sendo vedado o fornecimento dessas informações a terceiros e a utilização de login e senha de outros Servidores.

Art. 7º As senhas não devem:

I - ser anotadas ou armazenadas em arquivos eletrônicos compreensíveis por linguagem humana (não criptografados);

II - ser baseadas em informações pessoais, como o próprio nome, nome de familiares, data de nascimento, endereço, placa de veículo, nome da empresa, nome do setores e não devem ser constituídas de combinações óbvias de teclado, como “abcdefgh”, “87654321”, entre outras.

Art. 8º É obrigatória a troca das senhas iniciais dadas pelo Setor de Informática, sendo de responsabilidade do usuário a troca periódica da senha criada.

Art. 9º Fica proibido a qualquer usuário trabalhar em equipamentos de informática autenticado (logado) como administrador ou com contas que tenham privilégios semelhantes, exceto quando autorizado pelo Setor de Informática.

Art. 10 Para cumprimento dos arts. 6º e 7º o Setor de Informática fornecerá orientações para os acessos aos equipamentos de autenticação, login/senha na rede de computadores da Câmara.

CAPÍTULO IV
DO ACESSO DOS USUÁRIOS À INTERNET

Art. 11. O acesso à Internet será autorizado para os usuários que necessitarem da mesma para o desempenho das suas atividades profissionais na Câmara de Vereadores, sendo vedado o acesso a endereços eletrônicos que não contenham informações que agreguem conhecimento profissional e/ou que não sejam para a finalidade da Câmara de Vereadores.

Parágrafo único. O uso da Internet será monitorado pelo Setor de Informática com a emissão de relatórios que, quando solicitados, informarão qual usuário está conectado, quando usou a Internet e qual página acessou.

Art. 12. A navegação será monitorada através de software de filtro de conteúdo que automaticamente realizará bloqueios de conteúdos inadequados.

Art. 13. A definição do art. 11, sobre a permissão para uso, navegação da internet, é de atribuição do Presidente da Mesa Diretora, sendo proibidos os acessos de sites:

I - de conteúdo pornográfico;

II - do tipo Proxy, que permitem aos usuários navegar na Internet de forma anônima;

III - de transmissão pela Internet de filmes e músicas como Netflix, Globo Play, Spotify e similares;

IV - de redes sociais, exceto quando seu uso for pertinente às atividades de interesse da Câmara de Vereadores;

V - de jogos;

VI - de violência;

VII - que defendam atividades ilegais;

VIII - que menosprezem, depreciem ou incitem o preconceito a determinadas classes, gêneros ou etnias;

IX - que permitam a transferência, downloads de arquivos e/ou programas ilegais;

X - que degradem a imagem da Câmara de Vereadores de Dilermando de Aguiar;

XI - que representem ameaça à segurança e integridade dos arquivos armazenados nos equipamentos da Casa.

XII - que acarretem lentidão à rede prejudicando o andamento do trabalho dos demais Servidores.

Art. 14. A liberação de acessos a sites e serviços não autorizados, mas necessários ao desempenho das atribuições da função, dependerá de prévia solicitação do interessado e de análise do Setor de Informática juntamente com a Mesa Diretora.

Art. 15. O Setor de Informática não se responsabiliza pelo vazamento de dados pessoais tais como senhas, número de contas e qualquer tipo na rede da Câmara de Vereadores devido à má utilização da Internet ou acesso a sites não confiáveis;

CAPÍTULO V
DO USO DE SOFTWARES E EQUIPAMENTOS DE INFORMÁTICA
Seção I
Dos Softwares

Art. 16. Os softwares de Gestão Pública e Serviços são os sistemas de informação que garantem o fluxo dos documentos e ações dos setores administrativos da Casa, por meio dos softwares de gestão contábil, gestão de compras, licitações e contratos, gestão de pessoas como recursos humanos e folha de pagamento, gestão de patrimônio, portal da transparência, legislativo e administrativo.

Art. 00. Em virtude da complexidade e especificidade dos softwares de gestão pública e serviços para o setor público, fica autorizada a contratação, pela devida modalidade do processo licitatório, de empresas terceirizadas prestadoras de serviço no setor público.

Art. 00. Os softwares contratados devem ser desenvolvidos e utilizados preferencialmente em ambiente Web e estarem disponíveis de forma remota, em tecnologia conhecida como “nuvem de dados”, com infraestrutura de data center adequado para garantir a segurança das informações e continuidade do serviço.

Art. 00. Compete à empresa contratada realizar os serviços de instalação, migração de dados, parametrização, implantação, treinamento, provimento de data center, manutenção legal, corretiva e tecnológica, e suporte técnico aos usuários.

Art. 00. Os servidores de banco de dados, de aplicativos e de firewall deverão ser dimensionados para atendimento satisfatório das demandas da Casa, conforme termo de referência desenvolvido pelo setor de informática.

Art. 00. Os softwares necessários para execução dos sistemas nos servidores da contratante, tais como Servidor Web, Banco de Dados, e outros necessários para execução do software da Câmara de Vereadores, devem ser compatíveis com sistemas operacionais existentes.

Art. 00. Nos contratos deverão estar prevista a permissão para o setor de informática acessar a todo banco de dados e programas mantidos em data center da contratante, para que a Casa possa realizar download sempre que necessário.

Art. 00. Fica instituída a possibilidade de substituição dos documentos em papel para documentos eletrônicos com assinatura digital, a partir dos arquivos gerados pelos softwares de gestão pública.

Art. 00. A Casa deverá utilizar preferencialmente softwares livres para provimento de seus sistemas de informação, com exceção dos softwares de gestão pública e serviços.

Art. 00. A Câmara de Vereadores utilizará os sistemas operacionais preferencialmente em softwares livres para elaboração de documentos, planilhas e apresentações de slides em plataforma livre e principalmente os sistemas relacionados aos processos legislativos e administrativos.

Art. 00. Compete ao setor de informática dar apoio operacional, tecnológico e suporte aos usuários para viabilizar a utilização dos softwares livres mantidos na Casa.

Art. 00. O servidor de e-mail oficial poderá ser provido e executado por empresa de notória idoneidade e especialização técnica, preferencialmente de forma gratuita, e os dados devem estar armazenados e seguir rigorosos controles de segurança, autenticidade, integridade, disponibilidade e armazenamento das informações.

Art. 00. As políticas de softwares livres serão incentivas, no âmbito da Casa, para dar provimento em soluções de tecnologias da informação e comunicação em que garantam o desenvolvimento de soluções tecnológicas livres e não proprietárias.

Art. 16. Por questões de padronização e segurança:

I - toda homologação de softwares ou sistemas de terceiros passará pelo Setor de Informática;

II - os acessos a bancos de dados da Câmara de Vereadores, para leitura e gravação, serão executados somente através de sistemas de gestão homologados, diretamente por técnicos de empresas terceirizadas devidamente autorizados.

Art. 17. É de responsabilidade dos usuários dos sistemas administrativos a atualização de informações e operação dos sistemas, bem como a responsabilidade sobre relatórios emitidos e a confidencialidade das informações registradas.

Art. 18. O Setor de Informática deverá participar de todas as ações de planejamento e modernização de rotinas, independentemente dos assuntos, referentes à aquisição e uso de softwares de terceiros e compras de equipamentos específicos.

Art. 19. As aquisições de bens, serviços e softwares de informática deverão ser avaliadas e homologados pelo Setor de Informática.

Art. 20. O Setor de Informática não prestará qualquer tipo de suporte/manutenção a equipamentos/sistemas/softwares que não tiverem sido avaliados anteriormente pela mesma durante sua aquisição e poderá removê-los a qualquer momento devolvendo aos seus proprietários.

Art. 21. Não serão instalados nos computadores da Câmara de Vereadores aplicativos que não visem o objetivo da função pública, como:

I - jogos;

II - players de música;

III - softwares de downloads;

IV - softwares para criação, emissão, manutenção ou gerenciamento de serviços tais como de investimentos financeiros, comércio eletrônico ou similares.

Art. 22. Serão priorizados os softwares de código aberto aos de código privado, quando houver a necessidades da busca de um novo aplicativo para o desempenho da função pública junto a Câmara de Vereadores.

Art. 23. A rede da Câmara de Vereadores será unificada fisicamente, com hubs, switches, cabos e logicamente com um único domínio.

Art. 24. Fica proibido alterar as configurações dos equipamentos, salvo mediante autorização expressa, justificada por escrito e com procedimento posterior executado pelo Setor de Informática.

Art. 25. Ficam proibidas as conexões e/ou desligamentos de energia elétrica e de dados lógicos em quaisquer equipamentos de informática da Câmara de Vereadores ou de empresas terceirizadas sem o conhecimento prévio e o acompanhamento do Setor de Informática, ou de quem este determinar, devendo o Setor ser comunicado com antecedência para que os técnicos realizem a desconexão dos equipamentos e, após o setor providenciar o transporte dos mesmos para os locais de destino, os técnicos deverão novamente ser comunicados para proceder com as ligações e instalações necessárias.

Art. 26. A utilização dos equipamentos e suprimentos de informática deve limitar-se exclusivamente às atividades inerentes ao serviço da Câmara de Vereadores.

Art. 27. Em hipótese alguma serão permitidas conexões de equipamentos particulares à rede de trabalho da Câmara de Vereadores.

Parágrafo Único. Constitui exceção ao caput o fornecimento de acesso a rede Wi-fi com o fornecimento de login e senha para utilização nas dependências da Câmara de Vereadores.

Art. 28. Os sistemas e computadores devem ter versões do software antivírus instaladas, ativadas e atualizadas permanentemente, cabendo ao usuário, em caso de suspeita de vírus ou problemas na funcionalidade, acionar o departamento técnico responsável mediante registro de chamado.

Art. 29. Documentos imprescindíveis para as atividades da Casa deverão ser salvos em drives de rede, sendo que tais arquivos, se gravados apenas localmente nos computadores não terão garantia de backup e poderão ser perdidos caso ocorra uma falha no computador, sendo, portanto, de responsabilidade do próprio usuário.

Art. 30. É vedada a abertura ou o manuseio de computadores ou outros equipamentos de informática para qualquer tipo de reparo que não seja realizado por um técnico devidamente contratados para o serviço.

Art. 31. Todos os modems internos ou externos serão removidos ou desativados pelo Setor de Informática para impedir a invasão/evasão de informações, programas, vírus, sendo que, em alguns casos especiais, conforme regra específica, será considerada a possibilidade de uso para planos de contingência mediante a autorização dos gestores das áreas e da área de informática.

Art. 32. É proibido o uso de computadores e recursos tecnológicos da Câmara de Vereadores para:

I - tentar ou obter acesso não autorizado a outro computador, servidor ou rede;

II - burlar quaisquer sistemas de segurança;

III - acessar informações confidenciais sem explícita autorização do proprietário;

IV - vigiar secretamente por dispositivos eletrônicos ou softwares, como, por exemplo, analisadores de pacotes (sniffers);

V - interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;

VI - usar qualquer tipo de recurso tecnológico para cometer ou ser cúmplice de atos de violação, assédio sexual, perturbação, manipulação ou supressão de direitos autorais ou propriedades intelectuais sem a devida autorização legal do titular;

VII - hospedar pornografia, material racista ou qualquer outro que viole a legislação em vigor no país, a moral, os bons costumes e a ordem pública;

CAPÍTULO VI
DA RESPONSABILIDADE DAS COORDENAÇÕES

Art. 33. Fica sob responsabilidade da Mesa Diretora a divulgação, aplicação e zelo da política de segurança, bem como, a aplicação das punições nela prevista.

CAPÍTULO VII
DA MONITORAÇÃO DOS USUÁRIOS E ACESSOS À INTERNET

Art. 34. O Setor de Informática será responsável pela realização dos processos de fiscalização e auditoria para garantir o cumprimento destas normas, com as ferramentas e tecnologias disponíveis.

Art. 35. O monitoramento dos usuários será feito por meio de registros de acesso (logs) realizados nos acessos à internet nas bancadas e salas de rede da Câmara de Vereadores.

Art. 36. Os bloqueios de navegação serão realizados através de software de filtro de conteúdo.

CAPÍTULO VIII
DO USO DO CORREIO ELETRÔNICO

Art. 37. Os usuários que utilizem uma conta de e-mail institucional, seja com o nome do usuário ou do setor pelo qual é responsável ou que o represente, deverão fazer uso do sistema de correio eletrônico disponibilizado pelo Setor de Informática como ferramenta oficial de envio e recebimento de e-mails relacionados às atividades de sua função, sendo esse também de acesso diário obrigatório.

Art. 38. O e-mail oficial ou correio eletrônico é a forma de comunicação oficial para transmissão de documentos com assinatura digital admitido no âmbito externo da Câmara de Dilermando de Aguiar com a finalidade de comunicação oficial entre os Servidores e Vereadores do Poder Legislativo que podem utilizar a extensão de e-mail @dilermandodeaguiar.rs.leg.br, não sendo permitida a utilização de qualquer outra extensão de e-mail para fins de comunicação oficial.

Art. 39. A infraestrutura dos e-mails oficiais é administrada pelo Setor de Informática e a inclusão ou exclusão das contas dos e-mails oficiais dos Servidores e Vereadores devem ser feitas mediante credenciamento prévio e por meio de termo de responsabilidade assinado pelo usuário, pelo responsável do setor de informática e pela Presidência da Mesa Diretora, e o termo deverá constar as datas iniciais e finais da utilização do e-mail, além das informações de responsabilidade da utilização do e-mail pelo usuário.

I – a senha do e-mail oficial é sigilosa e intransferível e a responsabilidade de preservar o sigilo e atualizar a senha é exclusiva de cada usuário, em conformidade com o termo de responsabilidade assinado pelo usuário;

II - qualquer irregularidade, falha no sistema ou risco de uso indevido do e-mail, devem ser imediatamente comunicados pelo usuário ao Setor de Informática, não sendo admitida, em nenhuma hipótese, a alegação, pelo usuário, de uso indevido da sua respectiva conta de e-mail oficial e/ou do uso indevido da sua respectiva assinatura digital, nos termos da legislação federal vigente e do termo de responsabilidade assinado pelo usuário;

III - a forma e estrutura dos e-mails são flexíveis, entretanto, deve-se evitar o uso de linguagem incompatível com uma comunicação oficial.

Art. 38. O uso da conta de e-mail e da ferramenta de correio eletrônico oficial disponibilizada deverá ser exclusiva para as funções exercidas na Câmara de Vereadores.

Art. 39. Para preservação das informações de interesse da Câmara de Vereadores, é proibido o uso de contas de e-mails pessoais para envio ou recebimento de mensagens relacionadas às atividades legislativas.

Art. 40. Fica proibido o uso de softwares de e-mail como Thunderbird e Evolution para envio ou recebimento de e-mails, exceto nos casos de extrema necessidade, que deverão ser analisados antecipadamente pelo Setor de Informática.

Art. 41. É proibido aos Vereadores e Servidores utilizar o correio eletrônico da Câmara de Vereadores para:

I - enviar qualquer mensagem por meios eletrônicos que torne seu remetente e/ou a Casa vulneráveis a ações civis ou criminais;

II - divulgar informações não autorizadas ou imagens de tela, sistemas, documentos e afins sem autorização expressa e formal concedida pelo proprietário desse ativo de informação;

III - falsificar informações de endereçamento, adulterar cabeçalhos para esconder a identidade de remetentes e/ou destinatários, com o objetivo de evitar as punições previstas;

IV - apagar mensagens pertinentes de correio eletrônico quando a Câmara de Vereadores estiver sujeita a algum tipo de investigação.

Art. 42. É proibido utilizar o serviço de correio eletrônico para propagar conteúdos que:

I - contenham qualquer ato ou forneça orientação que conflite ou contrarie os interesses da Câmara de Vereadores;

II - contenha arquivos com código executável, tais como .exe, .com, .bat, .pif, .js, .vbs, .hta, .src, .cpl, .reg, .dll, .inf ou qualquer outra extensão que represente um risco à segurança;

III - visem obter acesso não autorizado a outro computador, servidor ou rede;

IV - visem interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;

IV - visem burlar qualquer sistema de segurança;

VI - visem vigiar secretamente ou assediar outro usuário;

VII - visem acessar informações confidenciais sem explícita autorização do proprietário;

VIII - visem acessar indevidamente informações que possam causar prejuízos a qualquer pessoa;

IX - incluam imagens criptografadas ou de qualquer forma mascaradas, salvo quando as atribuições da atividade assim o exigirem;

X - violem a lei, a moral, os bons costumes, a propriedade intelectual, os direitos à honra, à vida privada, à imagem, à intimidade pessoal e familiar;

XI - estimulem a prática de condutas ilícitas ou contrárias à moral e aos bons costumes;

XII - incitem a prática de atos discriminatórios, seja em razão de sexo, raça, religião, crenças, idade ou qualquer outra condição;

XIII - possibilitem o acesso a mensagens, produtos ou serviços de conteúdo ilícito, violento, pornográfico e/ou degradantes;

XIV - violem o sigilo das comunicações;

XV - veiculem, incitem ou estimulem a pedofilia;

XVI - incorporem vírus, spam ou outros elementos físicos ou eletrônicos que possam danificar ou impedir o normal funcionamento da rede, do sistema ou dos equipamentos informáticos (hardware e software) ou de terceiros;

XVII - encorajem conduta que possa consistir uma ofensa criminal, dar margem à responsabilidade civil ou ainda violar qualquer lei ou regulamento local, estadual, nacional ou internacional;

XVIII - tentem obter acesso ilegal a bancos de dados ou sistemas em geral;

XIX - alterem e/ou copiem arquivos ou ainda obtenham senhas e dados de terceiros sem prévia autorização.

CAPÍTULO IX

DAS PENALIDADES

Art. 43. O Setor de Informática fica responsável por relatar formalmente ao Presidente da Mesa Diretora que houve infração da política de segurança.

Art. 44. A inobservância das normas implicará na aplicação das penalidades previstas no regime jurídico dos Servidores públicos do Município, resguardado o exercício da ampla defesa e do contraditório em eventual processo administrativo.

Art. 45. Esta Resolução entra em vigor na data de sua publicação.

JUSTIFICATIVA A RESOLUÇÃO Nº. 000/2022

CONSIDERANDO a grande popularização da internet, a utilização de novas tecnologias e a necessidade de cada vez mais estar conectado;

CONSIDERANDO a necessidade de uma política que vise a segurança e proteção dos dados, equipamentos e todo o ambiente onde a informática está inserida;

CONSIDERANDO que a missão do Setor de Tecnologia da Informação é fornecer suporte às atividades finalísticas da Câmara e manter um ambiente apropriado para o funcionamento de softwares, serviços e dados corporativos, provendo aos usuários as ferramentas tecnológicas necessárias para o desempenho de suas funções primando pela segurança e zelo sobre os dados.

Avenida Ibicuí, S/N, CEP: 97.180-000, CNPJ: 01.679.377/0001-81,
one: 55 3612 4252, http://dilermandodeaguiar.rs.leg.br, camara@dilermandodeaguair.rs.leg.br

ANEXO I

Manual das práticas de privacidade e segurança da informação

1. OBJETIVO

Esta política de segurança da informação tem como principal objetivo documentar e proteger as informações consideradas importantes para a continuidade e manutenção dos objetivos dos serviços desenvolvidos na Câmara de Vereadores de Dilermando de Aguiar e é realizada com o fim de atender os princípios básicos da segurança da informação, conhecidos pelo acrônimo CID: confidencialidade, integridade e disponibilidade.

2. ABRANGÊNCIA

Todos os Vereadores, Servidores, fornecedores, visitantes e pessoas de modo geral que possuem alguma troca de informações com a Câmara de Vereadores.

3. DEFINIÇÕES

Esse manual deve ser divulgado a todos os Vereadores, Servidores e envolvidos de alguma forma com a Casa, e não abrange somente os sistemas computacionais, o conceito deve ser aplicado a todos os aspectos de proteção relacionada a tecnologia, procedimentos e pessoas.

4. ACESSO À INFORMAÇÃO

4.1. Política de Senhas

A senha é a forma mais convencional de identificação de acesso do usuário, e é um recurso pessoal e intransferível que protege a identidade dos usuários autorizados.

Por conta disso, abaixo seguem algumas regras que devem ser seguidas para elaboração de senhas seguras:

a) a senha é de total responsabilidade do usuário, sendo expressamente proibida sua divulgação ou empréstimo, devendo ser imediatamente alterada no caso de suspeita de divulgação;

b) b senha inicial só será fornecida ao próprio usuário, que deverá efetuar sua alteração para que tenha acesso aos sistemas;

c) é proibido o compartilhamento de login para funções de administração dos sistemas;

d) as senhas não devem ser anotadas em agendas pessoais;

e) é proibido o compartilhamento de senha com terceiros fora da Câmara de Vereadores;

f) é proibido utilizar a senha em equipamentos de terceiros;

g) as senhas deverão seguir os seguintes pré-requisitos:

1. Tamanho mínimo de oito caracteres;

2. Possuir pelo menos 3 caracteres dos seguintes tipos: letras maiúsculas, letras minúsculas, números e caracteres especiais;

3. Não devem ser baseadas em informações pessoais de fácil dedução tais como data de aniversário, nome do pai, sequência numérica ou alfabética;

4. Recomenda-se que as senhas tenham validade máxima de 06 (seis) meses;

5. Não poderão repetir senhas anteriores (últimas 3 senhas).

h) o acesso do usuário deverá ser imediatamente cancelado nas seguintes situações:

1. Desligamento da Câmara de Vereadores;

2. Mudança de função dentro da Câmara de Vereadores;

3. Quando, por qualquer razão, cessar a necessidade de acesso ao sistema ou informação.

i) para os cancelamentos acima mencionados, a área de Recursos Humanos ficará responsável por informar prontamente a equipe do Setor de Informática acerca dos desligamentos e mudança de função dos usuários.

4.2. E-mail

O e-mail é uma das principais ferramentas de comunicação da Casa, porém é uma das principais vias de disseminação de malwares, vírus e Spam, sendo que por isso surge a necessidade de normatização de seu uso.

O e-mail corporativo da Câmara de Vereadores de Dilermando de Aguiar é destinado a fins profissionais, relacionados às atividades da Casa apenas;

Os e-mails enviados ou recebidos de endereços externos poderão ser monitorados com o intuito de bloquear spams, malwares, vírus ou outros conteúdos maliciosos que violem a Política de Segurança da Informação da Casa constante no Anexo III da resolução nº. 002/2022.

É proibido enviar, com endereço eletrônico da Câmara de Vereadores, mensagens com anúncios particulares, propagandas, vídeos, fotografias, músicas, mensagens do tipo corrente, campanhas ou promoções;

É proibido abrir arquivos com origens desconhecidas anexadas a mensagens eletrônicas;

É proibido falsificar informações de endereçamento, adulterar cabeçalhos para esconder a identidade de remetentes e/ou destinatários;

Produzir, transmitir ou divulgar mensagem que:

1. Contenha ameaças eletrônicas, como: spam, phishing, mail bombing, mailwares;

2. Contenha arquivos com código executável: .exe, .cmd, .pif, .js, .hta, .src, .cpl, .reg, .dll, .inf, ou qualquer extensão que represente risco à segurança;

3. Vise obter acesso não autorizado a outro computador, servidor ou rede;

4. Vise interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;

5. Vise burlar qualquer sistema de segurança;

6. Vise vigiar secretamente ou assediar qualquer pessoa que seja;

7. Vise acessar informações confidenciais sem explicita consentimento / autorização do titular;

8. Tenha conteúdo impróprio, obsceno ou ilegal;

9. Seja de caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pornográfico entre outros;

10. Inclua material protegido por direitos autorais sem a permissão do titular dos direitos;

11. Dados pessoais tanto de Vereadores / Servidores quanto de terceiros que preste serviços a Casa;

O uso de e-mails pessoais é aceitável, se usado com moderação, em caso de necessidade e quando:

1. Não contrariar as normas aqui estabelecidas;

2. Não interferir, negativamente, nas atribuições funcionais dos Servidores.

4.3. Acesso à Rede

O acesso à rede interna da Câmara de Vereadores deve ser devidamente controlado para que os riscos de acessos não autorizados e/ou indisponibilidade das informações sejam minimizados.

Por conta disso, é preciso que sejam instauradas algumas regras de privacidade, listadas abaixo:

A Internet sem fio deverá ser acessada utilizando usuário e senha de rede;

É proibido visitantes terem acesso a rede sem fio, para este tipo de acesso será disponibilizada uma rede específica que não terá conectividade com a rede local;

O uso, a cópia ou a distribuição não autorizada de softwares que tenham direitos autorais, marca registrada ou patente são expressamente proibidos;

Os Vereadores e Servidores não poderão utilizar os recursos da Câmara de Vereadores para fazer o download ou distribuição de software ou dados pirateados, atividade considerada delituosa de acordo com a legislação nacional;

Como regra geral, materiais de cunho sexual não poderão ser expostos, armazenados, distribuídos, editados, impressos ou gravados por meio de qualquer recurso;

Documentos digitais de condutas consideradas ilícitas, como por exemplo, apologia ao tráfico de drogas e pedofilia, são expressamente proibidos e não devem ser acessados, expostos, armazenados, distribuídos, editados, impressos ou gravados por meio de qualquer recurso;

Os Vereadores e Servidores não poderão usar os recursos da Câmara de Vereadores para deliberada ou inadvertidamente propagar qualquer tipo de vírus, worms, cavalos de troia, spam, ou programas de controle remoto de outros computadores;

Não serão permitidas tentativas de burlar os controles de acesso à rede, tais como utilização de proxies anônimos e estratégias de by-pass de firewall;

Não serão permitidos o uso de aplicativos de reconhecimento de vulnerabilidades, análise de tráfego, ou qualquer outro que possa causar sobrecarga ou prejudicar o bom funcionamento e a segurança da rede interna, salvo os casos em que o objetivo for realizar auditorias de segurança.

5. CLASSIFICAÇÃO DA INFORMAÇÃO

A classificação da informação consiste na definição de níveis de proteção que cada dado deve receber e serve para garantir que nenhum dado seja divulgado indevidamente e que apenas as pessoas que tem direito recebam acesso à informação.

A classificação da informação deverá estar alinhada com as definições da Resolução nº. 002/2022 que regulamenta a Lei Geral de Proteção de Dados na Casa, assim como seus manuais, que definem as normas de coleta, tratamento, proteção e publicação de dados pessoais e sensíveis.

5.1. Responsabilidade e princípios da classificação da informação

O Setor de Informática é o responsável por solicitar a classificação do sigilo das informações aos Vereadores e Servidores, sendo que essa classificação da informação deve levar em consideração:

1. A necessidade de proteger as informações de acordo com sua importância e suas consequências, caso estas sejam comprometidas;
2. As regulamentações e exigências legais;
3. As obrigações contratuais.

A classificação da informação deve existir independentemente do formato, local e da mídia de armazenamento;

As concessões de acesso aos ambientes computacionais, pastas de rede, dispositivos de rede e outros que possibilitem acesso às informações da Câmara de Vereadores, devem ter aprovação do Comitê Gestor de Dados instituído pelo Resolução nº. 001/2022;

O Setor da Informática e o Comitê Gestor de Dados deve realizar periodicamente um processo de análise de classificação, para avaliar se a informação permanece com o mesmo nível de sigilo ou se deve ser solicitada sua reclassificação.

Os direitos de acesso dos Vereadores e Servidores às informações devem ser periodicamente revistos e atualizados e nos casos em que houver a combinação de várias informações diferentemente classificadas, as informações resultantes devem ser classificadas adotando-se o nível de classificação mais alto de restrição.

5.2. Níveis de classificação

A designação do nível de segurança de uma determinada classificação constitui o marco inicial que vai possibilitar determinar as salvaguardas mínimas necessárias para proteger informações sensíveis e garantir a continuidade operacional crítica da capacidade de processamento das informações.

Para isso devemos seguir a seguinte classificação com relação as informações:

Confidencial: é o nível mais alto de segurança dentro deste padrão, as informações confidenciais são aquelas que, se divulgadas interna ou externamente, tem potencial para trazer grandes prejuízos financeiros ou a imagem da Casa. Portanto, nessa classificação incluem-se todos os dados pessoais e sensíveis definidos na planilha de Inventário de Dados constante do Anexo I da Resolução nº. 002/2022 da Casa.

Confidencial-DP: é uma subclassificação da classificação Confidencial para dados pessoais e/ou sensíveis (DP) para dar tratamento adequado e, seguir os processos destinados a DP, conforme LGPD;

Restrita: é o nível médio de confidencialidade onde constam informações estratégicas que devem estar disponíveis apenas para usuários previamente autorizados;

Uso interno: representa baixo nível de confidencialidade o qual traz informações de uso interno que são aquelas em que não podem ser divulgadas para fora da Câmara de Vereadores, mas que, caso isso aconteça, não causarão grandes prejuízos.

Pública: são aqueles informações que não necessitam de proteção sofisticada contra vazamentos, pois podem ser de conhecimento público, tais como as informações constantes no Portal da Transparência da Casa.

5.3. Ciclo de vida da informação

O ciclo de vida da informação corresponde aos momentos vividos pela informação e que são evidentes quando os ativos físicos, tecnológicos e humanos fazem uso da informação, garantindo processos que suportam a operacionalização dos serviços da Câmara de Vereadores de Dilermando de Aguiar.

Neste sentido, o ciclo de vida da informação merece atenção, pois corresponde às situações em que a informação é exposta a ameaças, colocando em risco sua integridade.

Por conta disso, podemos destacar quatro fases relativas ao ciclo de vida:

1ª Fase: quando a informação é criada e manipulada, seja ao folhear papéis, digitar informações recebidas ou até mesmo o uso de senha de acesso para autenticação;

2ª Fase: quando a informação é armazenada, seja em banco de dados, anotações em papel, mídia ótica ou outro meio;

3ª Fase: quando a informação é transportada, seja por e-mail ou outra forma de compartilhamento de dados;

4ª Fase: quando a informação já não é mais útil e deve ser descartada ou depositada em uma lixeira, apagada do banco de dados.

O nível de classificação poderá mudar durante o ciclo de vida, de forma que uma informação "confidencial" poderá ser considerada "restrita" posteriormente, por exemplo, desde que o Comitê Gestor de Dados assim estabeleça, respeitando o ciclo de vida da reclassificação e as normas prevista na Resolução nº. 005/2019 que trata do arquivo público da Casa.

5.4. Boas Práticas

É preciso atenção especial para evitar que informações sensíveis não sejam solicitadas erroneamente, como classificação pública, de forma que devem ser adotados critérios para se decidir quais informações podem ser classificadas como públicas;

As informações de caráter confidencial devem ter sua classificação estabelecida na planilha de inventário de dados constante do Anexo I da Resolução nº. 002/2022;

As informações que não possuírem classificação de forma explícita, não eximem o Comitê Gestor da informação da responsabilidade de avalia-las e solicitar para que sejam classificadas adequadamente;

A utilização e o acesso das informações produzidas ou recebidas devem ser feitos de acordo com sua classificação, atribuindo aos respectivos usuários as permissões mínimas necessárias ao desempenho de suas atividades;

O processamento, armazenamento, transmissão e eliminação da informação devem ser feitos de acordo com sua classificação, nos moldes da legislação vigente em especial a Resolução nº. 005/2019 e a Resolução nº. 002/2022;

O armazenamento da informação deve considerar medidas de proteção lógica e física, de acordo com sua classificação, de forma que a informação seja acessada apenas por usuários autorizados;

A eliminação da informação deve ocorrer de forma permanente, seguindo procedimentos determinados, e que podem abranger a utilização de fragmentadores de papel, desmagnetizadores de disco rígido, dentre outros recursos;

A informação deve ser classificada antes de ser divulgada / compartilhada com terceiros e após o consentimento do titular, se houver, sob o risco de perder o caráter sigiloso, se for o caso.

6. CONSCIENTIZAÇÃO E TREINAMENTO

O objetivo é que todos os Vereadores e Servidores da Casa tenham um nível adequado de conhecimento sobre segurança, além de um senso apropriado de responsabilidade, pois é preciso sempre estimulando e motivando-os a se preocuparem com a segurança e privacidade dos dados e seu compartilhamento.

Deve fazer parte do cronograma de treinamento da Casa no Plano Estratégico existente, treinamentos específicos sobre segurança da informação e Lei Geral de Proteção de Dados, a fim de manter um controle de quantos participaram de treinamentos, visto que novos Vereadores e Servidores podem chegar todos os anos.

Além dos treinamentos e manuais, boletins informativos de boas práticas devem ser utilizados constantemente para fixar os itens mais importantes.

7. CONTINUIDADE DO SERVIÇO PÚBLICO

O processo de gestão de continuidade do serviço público relativo a segurança da informação, é implementado para minimizar os impactos e recuperar perdas de ativos da informação, após algum incidente crítico, retornando as rotinas a um nível aceitável, por meio da combinação de requisitos como operações, usuários chaves, mapeamento de processos críticos, análise de impacto e testes periódicos de recuperação.

Referido processo seguirá algumas regras estabelecidas no Plano Estratégico da Casa, devendo considerar, ao menos, os seguintes cenários para a realização de testes de continuidade do serviço público caso ocorram algum incidente:

1. Exploração de possíveis vulnerabilidades que permitam o acesso, a cópia e/ou a extração de informações e dados internos e/ou confidenciais do ambiente lógico da Câmara de Vereadores;

2. Realização de testes de intrusão a base de dados contendo informações sensíveis da Casa;

3. Tempo de recuperação de acesso a informações de backup em caso de perda de informações sensíveis;

4. Estratégias de recuperação de informações sensíveis e serviços relevantes;

Definição da quantidade de recursos mínimos a serem recuperados em caso de falha grave de perda de dados para que o serviço não seja interrompido.

8. ACESSO FÍSICO

Todo acesso físico à Câmara de Vereadores será identificado, de forma eletrônica ou manual para visitantes, levando em conta o sistema de câmeras de segurança existente nos pontos estratégicos e as gravações armazenadas em nuvem, retendo imagens por mínimo 25 dias.

Todos as informações produzidas deverão estar instalados no datacenter da empresa contratada para oferecimento de serviços de gestão pública, onde possui controle de acesso para apenas usuários previamente autorizados.

9. PLANO DE RESPOSTA A INCIDENTES

O plano de resposta a incidentes de segurança e privacidade é basicamente um processo no qual descreve como a Câmara de Vereadores irá responder às situações de emergência e exceções.

Temos que ter em mente que pela gravidade, a resposta deve ser rápida e confiável, ao mesmo tempo resguardando evidências forenses que possam ajudar a prevenir novos incidentes e atendendo as exigências legais de comunicação e transparência.

Assim, para o processo funcionar temos que nos ater aos seguintes pré-requisitos previamente e de forma contínua, atendendo os seguintes itens:

a) formação de uma Comissão, que poder ser a mesma indicado ao Comitê Gestor de Dados, designada por meio de Portaria do Presidente da Mesa com acessos, habilidades, responsabilidades, treinamento e conhecimentos para responder aos mais variados tipos de incidentes. Essa Comissão deve ter

reuniões periódicas para definir melhorias neste plano, verificação de pré-requisitos, mecanismos, atribuições, necessidade de preparo, bem como divulgação e treinamentos para os membros envolvidos juntamente com o encarregado pelo tratamento de dados pessoais;

b) instalação de divulgação dos mecanismos de comunicação de incidente as quais devem ser criadas, disponibilizadas e publicadas em forma de notificação a Câmara de Vereadores quando ocorrerem incidentes conforme determina a Resolução nº. 002/2022, a qual estabelece que a identidade e as informações de contato do encarregado deverão ser divulgadas publicamente, de forma clara e objetiva, preferencialmente no sitio eletrônico do controlador.

9.1. Processo de resposta a incidentes novos:

1. Um novo incidente é notificado, por pessoa externa ou não a Casa, sendo essa notificação recebida pelo Comitê Gestor da Casa.

9.2. Processo de triagem de incidentes:

1. O Comitê Gestor de Dados da Casa deve fazer a avaliação preliminar, descartando as notificações nulas ou claramente improcedentes, tomando os devidos cuidados;

2. Na avaliação preliminar, devem ser buscadas informações sobre os sistemas que foram alegadamente impactados, sua criticidade, quais os danos aparentes e o risco da situação se agravar se não houver resposta imediata;

3. Conforme a avaliação preliminar, incidentes que não envolvem sistemas online e que seguramente não apresentam riscos aumentados pela falha de ação imediata podem ser reencaminhados para tramites regulares do Comitê do e Encarregado, caso o incidente envolva dados pessoais;

4. Em caso de incidentes que exijam resposta imediata ou melhor avaliação, o Comitê Gestor de Dados deve passar para a fase de avaliação.

9.3. Processo de avaliação de incidentes:

1. Nesta fase deve ser iniciada uma avaliação mais detalhada do incidente no qual deve o Comitê Gestor buscar identificar a causa do incidente, endereços IP e credenciais envolvidas, transações e transferências de dados irregulares, métodos e vulnerabilidades exploradas, visando determinar ações para as demais fases.

9.4. Processo de contenção e erradicação de incidentes:

1. O objetivo das medidas de contenção e erradicação é limitar o dano e isolar os sistemas afetados para evitar mais transtornos e conforme a necessidade deverá ser obtida autorização para realizar o desligamento dos sistemas inteiros ou de funcionalidades específicas, assim como devem ser feitas comunicações de avisos de indisponibilidade para manutenção, sempre que possível tomando cuidados para

não impactar evidências que poderiam ser utilizadas para identificar autoria, origem e método usado para quebrar a segurança.

9.5. Processo de recuperação de incidentes:

1. Iniciar o plano de continuidade do serviço público imediatamente conforme especificado;

2. A recuperação é o conjunto de medidas para restaurar os serviços completamente, mas pode ser feita de forma gradual, conforme viabilidade e decisão da Mesa Diretora;

3. A Comissão do Comitê Gestor de Dados tem a responsabilidade de passar as informações que obteve para o desenvolvimento da solução e sua instalação;

4. Para a recuperação devem ser tomadas medidas identificadas na avaliação, tais como: restauração de backups, clonagem de máquinas virtuais, reinstalação de sistemas danificados;

5. Pode ser necessário o desenvolvimento e instalação de atualizações de aplicação ou do Sistema operacionais, por isso esta fase pode ser prolongada, de acordo com as prioridades dadas.

9.6. Processo de aprendizado com os incidentes:

1. Com o incidente contido e sua resolução encaminhada, a Comissão do Comitê Gestor de Dados deve agendar e conduzir uma reunião para apresentar o que ficou de aprendizado desse incidente, com convidados a seu critério, com o objetivo de discutir erros e dificuldades encontradas, propor melhorias para os sistemas e processos, inclusive deste plano de resposta a incidentes;

2. As melhorias sugeridas, com o devido consenso, devem ser encaminhadas a Mesa Diretora para definição sobre sua adoção.

9.7. Processo de documentação dos incidentes:

1. A Comissão do Comitê Gestor de Dados deve documentar o incidente em base de conhecimento apropriada, detalhando as informações obtidas, linha do tempo, atores envolvidos, evidencias, conclusões, decisões, autorizações e ações tomadas, inclusive as da reunião de aprendizados.

9.8. Processo de comunicação dos incidentes:

1. No caso de incidente com vazamento de dados pessoais, o Encarregado deve avaliar se há risco ou dano relevante aos titulares dos dados e deve fazer as comunicações obrigatórias previstas na Resolução nº. 002/2022, na maior brevidade possível, no máximo em até dois dias úteis, sendo que essas comunicações podem incluir agradecimentos ao notificador e/ou informações para os titulares dos dados