

PROJETO DE RESOLUÇÃO Nº , DE 2025.

“Institui a Política de Segurança da Informação – PSI da Câmara Municipal de Itanhaém.”

A MESA DIRETORA DA CÂMARA MUNICIPAL DE ITANHAÉM, no exercício de suas atribuições legais,

CONSIDERANDO ser fundamental proteger as informações que suportam a missão do Poder Legislativo Municipal;

CONSIDERANDO que a informação, em todo o seu ciclo de vida, constitui-se em bem estratégico e em ativo fundamental para o desempenho das atribuições constitucionais e para as atividades administrativas da Câmara Municipal de Itanhaém;

CONSIDERANDO a necessidade de aderência aos normativos existentes quanto ao acesso e à divulgação da informação, em especial a Lei Federal nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação);

CONSIDERANDO o disposto na Lei Federal nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados), alterada pela Lei Nacional nº 13.853, de 08 de julho de 2019;

CONSIDERANDO o disposto na Lei Federal nº 2.965, de 23 de junho de 2014 (Marco Civil da Internet);

CONSIDERANDO a necessidade de estabelecer princípios, objetivos, diretrizes e requisitos gerais que promovam a gestão integrada e coerente de processos voltados à segurança da informação, que sejam periodicamente revistos;

CONSIDERANDO a necessidade de instituir e manter uma política que norteie o tratamento de informações no âmbito da Câmara Municipal de Itanhaém, quanto

aos aspectos de segurança e a necessidade de aprimoramento contínuo da gestão da Segurança da Informação;

CONSIDERANDO a importância de manter e zelar pela integridade, disponibilidade e confidencialidade das informações corporativas como meio eficaz para a consolidação e transparência; e

CONSIDERANDO a necessidade de esclarecer e determinar aos usuários seus direitos e deveres no tocante à segurança da informação.

R E S O L V E:

SEÇÃO I

DISPOSIÇÕES GERAIS

Art. 1º Fica instituída a Política de Segurança da Informação (PSI) da Câmara Municipal de Itanhaém, Estado de São Paulo, com o objetivo de estabelecer diretrizes, normas e responsabilidades relacionadas à segurança da informação no âmbito desta Casa Legislativa.

Art. 2º A Política de Segurança da Informação (PSI) visa proteger a confidencialidade, integridade e disponibilidade das informações, bem como garantir a conformidade com a legislação vigente e minimizar riscos decorrentes do uso inadequado de informações e sistemas de informação.

Art. 3º Para os fins da PSI, entende-se como:

I- autenticação: processo pelo qual o usuário apresenta sua identificação ao recurso computacional para obtenção de acesso válido, podendo dar-se por senha, dispositivo de segurança (como token ou "chaveiro digital", ou cartão digital de acesso), biometria (impressão digital, palmar ou da íris), entre outros;

II- autenticidade: atributos que atestam a proveniência, a veracidade e a fidedignidade dos conteúdos informacionais;

III- ciclo de vida dos conteúdos informacionais: compreende, no todo ou em parte, as etapas de criação, formalização, captura, aquisição, tratamento,

armazenamento, preservação, recuperação, acesso, uso, disseminação, avaliação e destinação do conteúdo informacional da Câmara Municipal de Itanhaém;

IV- confidencialidade: qualidade de grau de sigilo, atribuído pela autoridade competente, a dados, informações ou documentos;

V- conteúdo informacional: toda informação registrada, produzida, recebida, adquirida, capturada ou colecionada pela Câmara Municipal de Itanhaém, no desempenho de sua missão institucional, qualquer que seja seu suporte;

VI- controle: forma de gerenciar o risco, incluindo políticas, procedimentos, diretrizes, práticas ou estruturas organizacionais, que podem ser de natureza administrativa, técnica, de gestão ou legal;

VII- disponibilidade: garantia de acesso à informação por usuários autorizados, quando necessário;

VIII- incidente de segurança da informação: evento simples ou série de eventos de segurança da informação indesejados ou inesperados, que tenham grande probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação;

IX- integridade: qualidade da informação que se encontra completa e que não sofreu nenhum tipo de dano ou alteração não autorizada ou não documentada, seja na origem, no trâmite ou na destinação;

X- registros de segurança: registros contendo atividades dos usuários, exceções e outros eventos de segurança da informação;

XI- risco: combinação da probabilidade de um evento e de suas consequências;

XII- segurança da informação: preservação da confidencialidade, integridade, disponibilidade e autenticidade da informação;

XIII- Sistema de Gestão da Segurança da Informação (SGSI): conjunto que compreende estrutura organizacional, políticas, atividades de planejamento, responsabilidades, práticas, procedimentos, processos, pessoas e demais recursos que a organização utiliza para, de modo coordenado e com base na abordagem de riscos, tratar os temas da segurança da informação; e

XIV- usuário: aquele que tem acesso autorizado aos conteúdos informacionais, em qualquer etapa de seu ciclo de vida, ou aos recursos de tecnologia da informação providos pela Câmara Municipal de Itanhaém, podendo ser vereador, servidor com qualquer tipo de vínculo, prestador de serviços terceirizado, estagiário, bem como pessoas física ou jurídica externas.

Art. 4º. As ações de Segurança da Informação devem buscar, alcançar e preservar os seguintes princípios:

- I-** Autenticidade: Garantia de que as informações e comunicações sejam genuínas, verificando a identidade de quem acessa ou altera os dados, e assegurando a origem e autoria das informações;
- II-** Confidencialidade: Garantia de que o acesso à informação seja restrito a pessoas autorizadas;
- III-** Disponibilidade: Garantia de que as informações e sistemas estejam acessíveis e utilizáveis quando necessário;
- IV-** Integridade: Garantia de que a informação seja mantida precisa e completa, preservando seu estado original;
- V-** Legalidade: Conformidade com as leis e normas aplicáveis, especialmente em relação à privacidade e proteção de dados pessoais.

SEÇÃO II

DOS PRINCÍPIOS E OBJETIVOS

Art. 5º São princípios da Política de Segurança da Informação:

- I-** a atenção e a responsabilidade de todos os usuários quanto à necessidade de segurança da informação;
- II-** a participação de todos, de modo a prevenir, detectar e responder aos incidentes de segurança da informação;
- III-** o respeito aos legítimos interesses dos usuários no acesso e uso da informação;
- IV-** a observância da publicidade como preceito geral e do sigilo como exceção;
- V-** a contínua análise dos riscos aos quais a informação está sujeita;
- VI-** a incorporação da segurança como requisito essencial dos sistemas de informação, informatizados ou não;
- VII-** a gestão sistêmica da segurança da informação;
- VIII-** a avaliação periódica da segurança da informação, de modo a realizar as modificações apropriadas a esta Política, bem como às práticas, demais normas e procedimentos de segurança da informação.

Art. 6º São objetivos da Política de Segurança da Informação:

- I- instituir uma cultura organizacional aderente à segurança da informação, compreendendo ações destinadas a fomentar entre os usuários a constante observância quanto às práticas destinadas à preservação dessa segurança;
- II- implantar a contínua avaliação dos riscos a que a informação está sujeita;
- III- estabelecer mecanismos que visem garantir a segurança da informação, em especial a confidencialidade, a integridade, a disponibilidade e a autenticidade nos projetos, processos e atividades da Câmara Municipal de Itanhaém;
- IV- implementar a governança da segurança da informação.

SEÇÃO III

DAS DIRETRIZES GERAIS

Art. 7º São diretrizes da Política de Segurança da Informação, no âmbito da Câmara Municipal de Itanhaém:

- I- alinhamento das ações de segurança da informação às atividades institucionais e às iniciativas estratégicas da Casa;
- II- capacitação adequada dos usuários frente às necessidades de segurança da informação;
- III- instituição de normas específicas e procedimentos para a segurança da informação aderentes a esta Política;
- IV- observância de leis, regulamentos e obrigações contratuais aos quais os processos de trabalho estão sujeitos, bem como normas e boas práticas, nacionais e internacionais, que sejam aplicáveis.

SEÇÃO IV

DAS RESPONSABILIDADES

Art. 8º Todos os usuários dos sistemas de informação e recursos tecnológicos da Câmara Municipal de Itanhaém, incluindo vereadores, servidores, colaboradores e prestadores de serviço, devem:

- I- Utilizar os recursos de TI de maneira responsável, garantindo a proteção das informações;
- II- Seguir as diretrizes da PSI, cumprindo as normas e procedimentos estabelecidos;
- III- Relatar qualquer incidente de segurança da informação ao Departamento de TI;
- IV- Respeitar as classificações de confidencialidade e integridade da informação;
- V- Proteger suas credenciais de acesso e não compartilhá-las;
- VI- Utilizar os sistemas e informações de maneira ética e conforme as normas internas;
- VII- Seguir as orientações do Departamento de TI sobre boas práticas de segurança da informação;
- VIII- Zelar pelos requisitos de confidencialidade, integridade, disponibilidades e autenticidade, no tocante aos conteúdos informacionais e aos recursos computacionais com os quais lidam;
- IX- Observar as normas e procedimentos relacionados à segurança da informação.

Art.9º O Departamento de Tecnologia da Informação (TI) será responsável pela:

- I- implementação, monitoramento e revisão periódica da PSI;
- II- Fornecer treinamento e orientação aos usuários;
- III- Assegurar a gestão adequada da segurança da informação, adotando controles e medidas preventivas;
- IV- Gerenciar o acesso aos sistemas e informações, de acordo com a necessidade de cada usuário;
- V- Garantir a proteção contra ameaças, como ataques cibernéticos, vírus e outras formas de invasão.
- VI- Planejar e coordenar as atividades relativas à Segurança da Informação;
- VII- Promover a divulgação das políticas, normas e melhores práticas de Segurança da Informação para todos os setores da Câmara Municipal de Itanhaém;
- VIII- Definir, promover e administrar, direta e indiretamente, modelos e métodos de gerenciamento que promovam segurança dos servidores de TIC;

IX- Realizar e acompanhar estudos de novas tecnologias para prevenir quanto a possíveis impactos na Segurança da Informação.

SEÇÃO V

DOS REQUISITOS

Art. 10 A Política de Segurança da Informação, no âmbito da Câmara Municipal de Itanhaém, atenderá aos seguintes requisitos:

- I-** Estabelecimento, manutenção e contínuo aprimoramento de um SGSI, devidamente documentado e adequado ao contexto das atividades da Casa e aos riscos que ela enfrenta;
- II-** Estabelecimento e aplicação de uma metodologia de análise e avaliação de riscos que dê suporte ao SGSI e que seja adequada aos requisitos legais, regulamentares e de segurança da informação identificados e aplicáveis à Casa;
- III-** Medição contínua da eficácia dos controles do SGSI para verificar se os requisitos de segurança da informação foram atendidos;
- IV-** Observância da proporcionalidade entre as medidas de segurança da informação implementadas e os riscos aos quais a informação está sujeita;
- V-** Exigência de competência e dos conhecimentos necessários para os usuários aos quais forem atribuídas responsabilidades definidas no SGSI;
- VI-** Orientação dos usuários quanto às práticas de segurança da informação.

CAPÍTULO VI

DA ADMISSÃO E EXONERAÇÃO DE SERVIDORES, TEMPORÁRIOS E ESTAGIÁRIOS

Art. 11 É necessária a comunicação ao Departamento de Tecnologia da Informação sobre todas as movimentações de colaboradores (servidores/estagiários/temporários/externos) dentro da Câmara Municipal de Itanhaém, desde que esses possuam acesso a qualquer ativo de informática (computadores, sistemas, softwares, contas de e-mail, logins, etc.).

Art. 12 Compete ao Departamento de Recursos Humanos informar ao Departamento de Tecnologia da Informação, a exoneração, o desligamento ou mudança de setor de colaboradores que possuam acesso a qualquer ativo de informática para o posterior bloqueio ou ajuste de seu tipo de acesso.

CAPÍTULO VI

DAS SENHAS E PERMISSÕES DE ACESSOS

Art. 13 Todo usuário terá seu próprio login e senha, fornecidos pelo Departamento de Tecnologia da Informação, para executar suas funções dentro da rede informatizada da Câmara Municipal de Itanhaém, 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 colaboradores.

Art. 14 As senhas não devem:

- I- Ser anotadas ou armazenadas em arquivos eletrônicos (Word, Excel, etc.), compreensíveis por linguagem humana (não criptografados);
- II- Ser baseadas em informações pessoais, como próprio nome, nome de familiares, data de nascimento, endereço, placa de veículo, nome da empresa, nome do departamento; e não devem ser constituídas de combinações óbvias de teclado, como “abcdefgh”, “87654321”, entre outras.

Art. 15 É obrigatória a troca das senhas iniciais dadas pelo Departamento de Tecnologia da Informação, sendo de responsabilidade do usuário a troca periódica da senha criada.

Art. 16 Fica proibido a qualquer usuário trabalhar em equipamentos de informática autenticado (logado) como administrador ou com contas que tenham privilégios semelhantes, exceto quando autorizado pela Departamento de Tecnologia da Informação.

Art. 17 Para cumprimento dos arts. 13º e 14º o Departamento de Tecnologia da Informação fornecerá orientações para os acessos aos equipamentos de autenticação (login/senha) na rede de computadores da Câmara Municipal de Itanhaém.

CAPÍTULO VII

DO ACESSO DOS USUÁRIOS À INTERNET

Art. 18. O acesso à Internet será autorizado para os usuários que necessitarem da mesma para o desempenho das suas atividades profissionais na Câmara Municipal de Itanhaém, sendo vedado o acesso a endereços eletrônicos que não contenham informações que agreguem conhecimento profissional e/ou para as atividades finalísticas da Câmara Municipal de Itanhaém.

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

Art. 19. A navegação será monitorada através de software de filtro de conteúdo que automaticamente realizará bloqueios de conteúdos inadequados.

Art. 20. A definição do art. 18, sobre a permissão para uso (navegação) da internet, é de atribuição dos Diretores entre Departamentos e Vereadores pelos Gabinetes da Câmara Municipal de Itanhaém, com base em recomendação do Departamento de Tecnologia da Informação, 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;
- IV-** De redes sociais, exceto quando seu uso for pertinente às atividades de interesse da Câmara Municipal de Itanhaém;
- 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 ou torrents) de arquivos e/ou programas ilegais;
- X-** Que degradem a imagem da Câmara Municipal de Itanhaém;
- XI-** Que representem ameaça à segurança e integridade dos arquivos armazenados nos equipamentos da Câmara Municipal de Itanhaém.
- XII-** Que acarretem lentidão à rede prejudicando o andamento do trabalho dos demais servidores.

Art. 21. A liberação de acessos a sites e serviços não autorizados, mas necessários ao desempenho das atribuições da função, dependerá de prévia solicitação da Diretoria do Departamento ou Gabinete interessado e de análise do Departamento de Tecnologia da Informação.

Art. 22. O Departamento de Tecnologia da Informação não se responsabiliza pelo vazamento de dados pessoais (senhas, número de contas, etc.) de qualquer tipo na rede da Câmara Municipal de Itanhaém devido à má utilização da Internet ou acesso a sites não confiáveis;

CAPÍTULO VIII

DO DIRETÓRIO NO SERVIDOR DE ARQUIVOS

Art. 23. Todos os Departamentos e Gabinetes de Vereador deverão ter espaço no servidor de arquivos, em forma de diretório, com limite de armazenamento de dados previamente definido pelo Departamento de Tecnologia da Informação.

Art. 24. O acesso ao diretório previsto no art. 22 será apenas para os usuários pertencentes ao mesmo Departamento ou Gabinete.

Art. 25. Caso haja a necessidade de se disponibilizar o acesso para usuários não pertencentes ao mesmo Departamento ou Gabinete, deverá ser aberto um chamado técnico para Departamento de Tecnologia da Informação, contendo a justificativa das Áreas envolvidas nesse procedimento.

Art. 26. Cada Departamento ou Gabinete será responsável pelo gerenciamento de seu diretório no servidor de arquivos, devendo ser apagados arquivos duplicados e arquivos sem utilidade.

Art. 27. Caso seja necessário manter arquivos duplicados e arquivos sem utilidade por mais tempo no diretório, deverá ser aberto um chamado para o Departamento de Tecnologia da Informação, a qual é responsável por realizar o backup do Servidor de Arquivos.

Art. 28. Todos os arquivos importantes e relacionados às atividades institucionais da Câmara Municipal de Itanhaém deverão ser armazenados em pasta compartilhada do Servidor de Arquivos, não no diretório local da estação de trabalho.

Art. 29. É proibida a produção, edição, distribuição ou exposição e armazenamento, nos sistemas de informação da Câmara Municipal de Itanhaém, de qualquer material que viole qualquer lei ou regulamentação em vigor no território nacional, tais como:

- I. Material de qualquer natureza que induza ou incite racismo, nazismo, discriminação ou preconceito de raça, cor, etnia, religião ou procedência nacional ou qualquer outro ato descrito pela legislação nacional como crime;
- II. Material protegido por copyright.
- III. Material cujo conteúdo esteja relacionado a sexo, drogas, pornografia, pedofilia, violência e armamento.
- IV. Marcas registradas.
- V. Segredo comercial ou qualquer direito de propriedade intelectual usado sem a devida autorização.
- VI. Material difamatório, que constitua uma ameaça ilegal à Câmara Municipal de Itanhaém ou a terceiros.

Art. 30. É também proibida a produção, edição, distribuição ou exposição e armazenamento, nos sistemas de informação da Câmara Municipal de Itanhaém, de qualquer material obsceno e de quaisquer materiais ou arquivos não relacionados às atividades institucionais da Câmara Municipal de Itanhaém.

Art. 31. Os equipamentos e o servidor de arquivos da Câmara Municipal de Itanhaém não poderão ser utilizados para desenvolvimento, distribuição e gravação de programas, aplicativos, filmes, vídeos, arquivos de áudio, executáveis e jogos, exceto os que forem relacionados às atividades desenvolvidas pela Câmara Municipal de Itanhaém e mediante prévia e expressa autorização da Presidência.

CAPÍTULO IX

DO ACESSO À REDE COM EQUIPAMENTOS PARTICULARES

Art. 32. O acesso à rede interna da Câmara Municipal de Itanhaém por meio de dispositivos particulares (como notebooks, smartphones e tablets) só será permitido mediante autorização expressa do Departamento de Tecnologia da Informação e sob as seguintes condições:

I - **Autenticação segura:** obrigatoriedade de credenciais individuais e uso de VPN (Rede Privada Virtual), quando aplicável;

II – **Atualização de segurança:** os dispositivos devem possuir sistemas operacionais e antivírus atualizados;

III – **Restrição de acesso:** limitação a redes e sistemas específicos, conforme necessidade funcional;

IV – **Proibição de armazenamento:** os usuários não poderão armazenar dados institucionais em dispositivos pessoais, salvo em ambientes previamente aprovados e criptografados.

Art. 33. Os equipamentos particulares conectados à rede da Câmara Municipal de Itanhaém estarão sujeitos a:

I – Monitoramento de atividades suspeitas;

II – Bloqueio imediato em caso de violação das políticas de segurança;

III – Auditorias eventuais para verificação de conformidade.

Parágrafo único. A Câmara Municipal de Itanhaém não se responsabiliza por danos, perdas ou vazamentos decorrentes do uso de dispositivos particulares.

CAPÍTULO IX

DO USO DE SOFTWARES E EQUIPAMENTOS DE INFORMÁTICA

Art. 34. Por questões de padronização e segurança:

I- Toda homologação de softwares ou sistemas de terceiros passará pelo Departamento de Tecnologia da Informação.

II- Os acessos a bancos de dados da Câmara Municipal de Itanhaém, para leitura e gravação, serão executados somente através de sistemas de gestão homologados, diretamente por técnicos de empresas terceirizadas devidamente autorizados ou pelos administradores do Departamento de Tecnologia da Informação.

Art. 35. 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. 36. O Departamento de Tecnologia da Informação deverá participar de todas as ações de planejamento e modernização de rotinas, independentemente dos assuntos (administrativos ou técnicos), referentes à aquisição e uso de softwares de terceiros e compras de equipamentos específicos.

Art. 37. As aquisições de bens, serviços e softwares de informática deverão ser avaliadas e homologados pelo Departamento de Tecnologia da Informação.

Art. 38. Não serão instalados nos computadores da Câmara Municipal de Itanhaém aplicativos que não visem o objetivo da função pública, como:

I- Jogos;

II- Players de música;

III- Softwares de torrent downloads;

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

Art. 39. A rede da Câmara Municipal de Itanhaém será unificada fisicamente (roteadores, switches e cabos) e logicamente (em um único Domínio).

Art. 40. Fica proibido alterar as configurações dos equipamentos, salvo mediante autorização expressa, justificada por escrito e com procedimento posterior executado pelo Departamento de Tecnologia da Informação.

Art. 41. Ficam proibidas as conexões e/ou desligamentos de energia elétrica e de dados lógicos em quaisquer equipamentos de informática da Câmara Municipal de Itanhaém ou de empresas terceirizadas sem o conhecimento prévio e o acompanhamento de um técnico do Departamento de Tecnologia da Informação, ou de quem está determinar, devendo o Departamento de Tecnologia da Informação ser comunicado com antecedência para que os técnicos realizem a desconexão dos equipamentos e, após o Departamento/Gabinete providenciar o transporte dos mesmos para os locais de destino, os técnicos do Departamento de Tecnologia da Informação deverão novamente ser comunicados para proceder com as ligações e instalações necessárias.

Art. 42. A utilização dos equipamentos e suprimentos de informática deve limitar-se exclusivamente às atividades inerentes ao serviço da Câmara Municipal de Itanhaém.

Art. 43. 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 de Tecnologia da Informação mediante registro de chamado técnico.

Art. 44. Documentos imprescindíveis para as atividades dos colaboradores da instituição deverão ser salvos em drives de rede, sendo que tais arquivos, se gravados apenas localmente nos computadores (por exemplo, no drive C:), não terão garantia de backup e poderão ser perdidos caso ocorra uma falha no computador, sendo, portanto, de responsabilidade do próprio usuário.

Art. 45. É vedada a abertura ou o manuseio de computadores ou outros equipamentos de informática para qualquer tipo de reparo que não seja realizado pelo Departamento de Tecnologia da Informação ou por terceiros devidamente contratados para o serviço.

Art. 46. É proibido o uso de computadores e recursos tecnológicos da Câmara Municipal de Itanhaém 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 outrem 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;
- VIII- utilizar software pirata, atividade considerada delituosa de acordo com a legislação nacional.

CAPÍTULO IX

DO MONITORAMENTO E DA AUDITORIA DO AMBIENTE

Art. 47. Para garantir as regras mencionadas nesta Resolução, o Departamento de Tecnologia da Informação poderá:

- I - implantar sistemas de monitoramento nas estações de trabalho, servidores, correio eletrônico, conexões com a internet, dispositivos móveis ou wireless e outros componentes da rede – a informação gerada por esses sistemas poderá ser usada para identificar usuários e respectivos acessos efetuados, bem como material manipulado;

II - tornar públicas as informações obtidas pelos sistemas de monitoramento e auditoria, no caso de exigência judicial ou solicitação do Diretor Geral ou Presidente da Câmara Municipal de Itanhaém;

III - realizar, a qualquer tempo, inspeção física nas máquinas de propriedade da Câmara Municipal de Itanhaém;

IV - instalar sistemas de proteção, preventivos e detectáveis, para garantir a segurança das informações e dos perímetros de acesso.

CAPÍTULO X

DO USO DO CORREIO ELETRÔNICO

Art. 48. Os usuários que utilizem uma conta de e-mail institucional, seja com o nome do usuário ou do departamento/gabinete pelo qual é responsável ou que o represente, deverão fazer uso do sistema de correio eletrônico disponibilizada pela Administração e pelo Departamento de Tecnologia da Informação como ferramenta oficial de envio e recebimento de e-mails relacionados às atividades de trabalho, sendo esse também de acesso diário obrigatório.

Art. 49. O uso da conta de e-mail e da ferramenta de correio eletrônico institucional disponibilizada deverá ser exclusiva para as funções exercidas na Câmara Municipal de Itanhaém.

Art. 50. Para preservação das informações de interesse da Câmara Municipal de Itanhaém, é proibido o uso de contas de e-mails pessoais para envio ou recebimento de mensagens relacionadas às atividades de trabalho.

Art. 51. É proibido aos servidores o uso do correio eletrônico da Câmara Municipal de Itanhaém:

- I- enviar qualquer mensagem por meios eletrônicos que torne seu remetente e/ou a Câmara Municipal de Itanhaém 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 Municipal de Itanhaém estiver sujeita a algum tipo de investigação.

Art. 52. É proibido utilizar o serviço de correio eletrônico para propagar conteúdos que:

I- conttenham qualquer ato ou forneça orientação que conflite ou contrarie os interesses da Câmara Municipal de Itanhaém;

II- contenha arquivos com código executável (.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;

V- 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 em 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 XI

DAS PENALIDADES

Art. 53 O Departamento de Tecnologia da Informação fica responsável por relatar formalmente ao Presidente da Câmara Municipal de Itanhaém a ocorrência de infração da política de segurança.

Art. 54 A inobservância das normas estabelecidas nessa Resolução implicará na aplicação das penalidades previstas na Lei nº 3.055/2004, que dispõe sobre o regime jurídico dos servidores públicos do Município de Itanhaém, resguardado o exercício da ampla defesa e do contraditório em eventual processo administrativo.

CAPÍTULO XII

DAS DISPOSIÇÕES TRANSITÓRIAS

Art. 55 O Departamento de Tecnologia da Informação, para elaboração e revisão de normas e procedimentos, terá como prioridade os seguintes temas, sem prejuízo de eventuais outras demandas:

- I- acesso, proteção e guarda da informação;
- II- aquisição, desenvolvimento e manutenção de sistemas informatizados;
- III- coleta e preservação de registros de segurança;
- IV- cópias de segurança de dados e de sistemas informatizados;
- V- gestão de incidentes de segurança da informação;

- VI-** inventário dos recursos computacionais e dos conteúdos informacionais, enfatizando os aspectos de responsabilidades, preservação e de uso aceitável;
- VII-** elaboração de Plano de Continuidade de Negócio;
- VIII-** segregação de ambientes de tecnologia da informação e comunicação, com a implementação de ambientes distintos de desenvolvimento, homologação e produção de sistemas computacionais, feitas em atendimento ao princípio da separação de funções, com a definição de papéis e responsabilidades, específicos para cada ambiente;
- IX-** segurança física das instalações e ambientes digitais que hospedam os conteúdos informacionais e os recursos computacionais para os quais essa normatização seja necessária.

Art. 56 Esta Resolução entra em vigor na data de sua publicação.

Sala “D. Idílio José Soares”, 1 de abril de 2025.

Edinaldo dos Santos Barros

Presidente da Câmara Municipal de Estância Balneária de Itanhaém

Fernando da Silva Xavier Miranda

1º Secretário da Câmara Municipal de Estância Balneária de Itanhaém

Severino Bento Gomes

2º Secretário da Câmara Municipal de Estância Balneária de Itanhaém

JUSTIFICATIVA

Senhores Vereadores:

O presente Projeto de Resolução, que visa instituir a Política de Segurança da Informação (PSI) da Câmara Municipal de Itanhaém, é de extrema importância para o fortalecimento da governança e proteção dos dados e informações no âmbito desta Casa Legislativa.

Em um cenário cada vez mais digital, onde o uso intensivo de sistemas de informação e recursos tecnológicos é essencial para o bom funcionamento das atividades legislativas e administrativas, a segurança da informação se apresenta como uma prioridade estratégica. A crescente troca de informações eletrônicas e a integração de sistemas tornam-se fatores críticos, o que exige a adoção de medidas de controle e gestão para garantir a integridade, confidencialidade, autenticidade e disponibilidade dessas informações.

A Política de Segurança da Informação estabelecida por este projeto tem como objetivo proteger os ativos de informação da Câmara Municipal, assegurando que os dados sejam tratados de acordo com os princípios legais e éticos, evitando riscos de acessos não autorizados, perda de dados, fraudes e outros incidentes que possam comprometer o funcionamento e a reputação da instituição.

Outro ponto relevante é a atribuição clara de papéis e responsabilidades, criando uma cultura institucional de segurança e conscientização. Isso irá promover a eficiência no uso de recursos de tecnologia da informação e comunicação (TIC), assim como a prevenção de incidentes de segurança que possam impactar negativamente as atividades legislativas e administrativas.

Portanto, a implementação da PSI irá contribuir significativamente para a mitigação de riscos, garantindo a proteção dos ativos de informação, a continuidade dos serviços, o cumprimento das normas legais e o aprimoramento das práticas de segurança no ambiente digital da Câmara Municipal.

Diante do exposto, a aprovação deste Projeto de Resolução se faz necessária e urgente, visando à modernização e proteção dos processos informacionais da Câmara Municipal de Itanhaém.

Câmara Municipal de Itanhaém, 1 de abril de 2025.

Edinaldo dos Santos Barros

Presidente da Câmara Municipal de Estância Balneária de Itanhaém

Fernando da Silva Xavier Miranda

1º Secretário da Câmara Municipal de Estância Balneária de Itanhaém

Severino Bento Gomes

2º Secretário da Câmara Municipal de Estância Balneária de Itanhaém

PROTOCOLO DE ASSINATURA(S)

O documento acima foi assinado eletronicamente e pode ser acessado no endereço /autenticidade utilizando o identificador 370035003500320033003A005000

Assinado eletronicamente por **SEVERINO BENTO GOMES** em 03/04/2025 09:19

Checksum: **B22E4551C1199DCEC855809C175BD8F4696215BA2C4B18807241ACBF7F9ABB28**

Assinado eletronicamente por **EDINALDO DOS SANTOS BARROS** em 03/04/2025 12:25

Checksum: **5E6DB7B0406FB82EA6E26ABC5B6A338BAD6A2346ADF56101D1A187DE9115CAD8**