RESOLUÇÃO Nº 281, DE 7 DE DEZEMBRO DE 2023

Projeto de autoria da Mesa

Institui a Política de Segurança da Informação da Câmara Municipal de Santa Isabel

A Câmara Municipal de Santa Isabel aprovou, e eu, LUIZ CARLOS ALVES DIAS, Presidente, promulgo a seguinte Resolução:

Seção I
Disposições Gerais

Art. 1º. Fica instituída a Política de Segurança da Informação da Câmara Municipal de Santa Isabel, com os seguintes objetivos:

I – definir diretrizes, responsabilidades, competências e princípios de Segurança da Informação – SI no âmbito da Câmara Municipal de Santa Isabel;

II – conduzir os setores da Câmara Municipal de Santa Isabel a níveis de risco gerenciáveis, no que diz respeito à segurança de suas informações;

III – garantir a disponibilidade, integridade, confidencialidade e autenticidade das informações que suportam as atividades e os objetivos estratégicos dos setores da Câmara Municipal de Santa Isabel;

IV – fomentar o comprometimento de todos os usuários dos conteúdos informacionais e dos recursos de tecnologia da informação providos pela Câmara Municipal de Santa Isabel, na implantação do Programa de Segurança da Informação;

V – disseminar a cultura da Segurança da Informação em todos os níveis organizacionais da Câmara Municipal de Santa Isabel.

Art. 2º. Para fins desta Resolução, considera-se:

I – Ameaça: evento que tem potencial em si próprio para comprometer os objetivos da organização, seja trazendo danos diretos aos ativos ou prejuízos decorrentes de situações inesperadas;

II – Ativo da informação: elementos que transformam, transportam, guardam e descartam dados ou informações, incluindo a própria informação, e que se dividem em 6 (seis) grupos:

a) equipamentos;
b) aplicações;
c) usuários;
d) ambientes;

e) dados; e

f) processos.

III – Autenticidade: garantia de que os ativos da informação identificados em um processo de comunicação como remetentes ou autores sejam exatamente quem diz ser;

IV – Confidencialidade: propriedade que garante que a informação só está disponível a indivíduos ou processos autorizados;

V – Dados: trata-se da informação não processada;

VI – Disponibilidade: propriedade que garante que a informação está disponível às pessoas e aos processos autorizados, a qualquer momento requerido;

VII – Grupo de Tratamento e Resposta a Incidentes: agentes responsáveis por receber, analisar e responder às notificações e atividades relacionadas a incidentes de Segurança da Informação;

VIII – Incidente de Segurança da Informação: é qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos ativos da informação;

IX – Informação: resultado do processamento, manipulação e organização de dados de tal forma que represente um acréscimo ao conhecimento da pessoa que a recebe, podendo se apresentar de diversas formas, como texto, imagem, áudio, etc.;

X – Integridade: propriedade que garante que a informação está intacta e protegida contra perda, dano ou modificação não autorizada;

XI – Recurso de TIC (Tecnologia da Informação e Comunicação): são os recursos tecnológicos que transformam, transportam, guardam e descartam dados ou informações;

XII – Risco: probabilidade de ameaças explorarem vulnerabilidades, comprometendo a confidencialidade, integridade ou disponibilidade da informação, causando impactos para um sistema ou organização;

XIII – Usuário: qualquer pessoa autorizada a ler, inserir ou atualizar informações;

XIV – Vulnerabilidade: fragilidade presente ou associada a um ativo ou grupo de ativos da informação, que pode ser explorada por uma ou mais ameaças, gerando incidentes de Segurança da Informação; e

XV – 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.

Art. 3º. As ações de Segurança da Informação devem buscar, alcançar e preservar os seguintes princípios:

I – autenticidade;

II – confidencialidade;

III – disponibilidade;

IV – integridade; e,

V – legalidade.

Seção II
Dos Princípios e Objetivos

Art. 4º. 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; e,

VIII – a avaliação periódica da segurança da informação, de modo tal a realizar as modificações apropriadas a esta Política, bem como às práticas, demais normas e procedimentos de segurança da informação.

Art. 5º. 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 Santa Isabel; e,

IV – implementar a governança da segurança da informação.

Seção III
Das Diretrizes

Art. 6º. São diretrizes da Política de Segurança da Informação, no âmbito da Câmara Municipal de Santa Isabel:

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; e,

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
Dos Requisitos

Art. 7º. A Política de Segurança da Informação, no âmbito da Câmara Municipal de Santa Isabel, 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.

Seção V
Da Implantação e Revisão da Política

Art. 8º. Fica criado o Comitê Gestor de Segurança da Informação (CGSI), composto por um servidor indicado como representante de cada uma das seguintes unidades administrativas da Casa:

I – Secretário Administrativo;

II – Responsável técnico pela Tecnologia da Informação – TI;

III – Assessoria Jurídica; e,

IV – Assessoria de Comunicação.

§1º. Cada representante será indicado com o respectivo substituto.

§2º. A coordenação do Comitê Gestor de Segurança da Informação (CGSI) caberá ao Secretário Administrativo.

§3º. Compete ao Comitê Gestor de Segurança da Informação:

I – avaliar periodicamente e manter atualizadas a Política de Segurança da Informação e as normas decorrentes;

II – demandar às unidades administrativas a elaboração de normas específicas relacionadas à segurança da informação em suas áreas de competência;

III – receber, avaliar e validar propostas de normas relativas à segurança da informação;

IV – encaminhar à autoridade competente para deliberação as propostas de atualização da política de segurança da informação e as propostas de normas correlatas;

V – coordenar a implantação e atualização do SGCI a ser elaborado pela Casa;

VI – acompanhar e avaliar o sistema implantado conforme o inciso anterior;

VII – coordenar a seleção, implantação e atualização da metodologia de análise periódica de riscos a ser adotada pela Casa, bem como a definição do escopo e abrangência dessas análises;

VIII – planejar e coordenar ações institucionais de segurança da informação; e,

IX – propor a inclusão das iniciativas relacionadas à segurança e preservação da informação nos planejamentos institucionais pertinentes e suas atualizações.

Art. 9º. O Comitê Gestor poderá convidar membros temporários para apoiá-los em suas atividades, de acordo com a necessidade.

Art. 10. Compete ao Secretário Administrativo:

I – supervisionar a implantação e execução da Política de Segurança da Informação da Câmara Municipal de Santa Isabel;

II – promover o envolvimento de todos os setores da Casa na consecução dos objetivos, diretrizes e requisitos desta Política.

Art. 11- Compete ao Secretário Administrativo com apoio do Responsável Técnico da Tecnologia da Informação – TI:

I – planejar e coordenar as atividades relativas à Segurança da Informação;

II – promover a divulgação das políticas, normas e melhores práticas de Segurança da Informação para todos os setores da Câmara Municipal de Santa Isabel;

III – promover a cultura de Segurança da Informação por meio de ações de sensibilização e conscientização;

IV – definir, promover e administrar, direta e indiretamente, modelos e métodos de gerenciamento que promovam segurança dos servidores de TIC (Tecnologia da Informação e Comunicação);

V – garantir os níveis de alinhamento das atividades de TIC (Tecnologia da Informação e Comunicação) a todas as políticas, normas e procedimentos de segurança estabelecidos;

VI – instituir e coordenar um Grupo de Tratamento e Resposta a Incidentes; e,

VII – realizar e acompanhar estudos de novas tecnologias para prevenir quanto a possíveis impactos na Segurança da Informação.

Art. 12. Compete à Assessoria de Comunicação e à Assessoria Jurídica:

I – planejar e coordenar a divulgação da política de segurança da informação, bem como as normas dela derivadas, e de suas atualizações; e,

II – elaborar pareceres, contratos e demais documentos jurídicos relativos à política de segurança da informação, bem como às normas derivadas, e de suas atualizações.

Art. 13. São atribuições dos usuários:

I – zelar pelos requisitos de confidencialidade, integridade, disponibilidade e autenticidade, no tocante aos conteúdos informacionais e aos recursos computacionais com os quais lidam;

II – observar as normas e procedimentos relacionados à segurança da informação.

Parágrafo Único. É dever do servidor comunicar à chefia imediata sobre violações identificadas em relação à Política prevista nesta Resolução e às normas e procedimentos dela decorrente.

Art. 14. São Direitos dos servidores, em relação à Política de Segurança da Informação:

I – receber treinamento adequado ao exercício de suas atribuições; e.

II – propor aperfeiçoamento da Política prevista nesta Resolução e de seus instrumentos de gestão.

Seção VI
Das Disposições Transitórias

Art. 15. O Comitê Gestor de Segurança da Informação, para elaboração e revisão de normas e procedimentos, terá como prioridade os seguintes temas, sem prejuízo de eventuais outras demandas:

I – gestores de sistemas de informação;

II – acesso, proteção e guarda da informação;

III – aquisição, desenvolvimento e manutenção de sistemas informatizados;

IV – classificação da informação;

V – coleta e preservação de registros de segurança;

VI – cópias de segurança de dados e de sistemas informatizados;

VII – gestão de incidentes de segurança da informação;

VIII – inventário dos recursos computacionais e dos conteúdos informacionais, enfatizando os aspectos de responsabilidades, preservação e de uso aceitável;

IX – elaboração de Plano de Continuidade de Negócio;

X – 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; e,

XI – segurança física das instalações e ambientes digitais que hospedam os conteúdos informacionais e os recursos computacionais para os quais essa normatização seja necessária.

Art. 16. Esta Resolução entra em vigor na data de sua publicação.

Santa Isabel, 7 de dezembro de 2023.

LUIZ CARLOS ALVES DIAS
Presidente

Registrada e publicada nesta Secretaria Administrativa, na data supra.

MARICÉLIA DOS SANTOS
Secretário Administrativo

VERIFICAÇÃO DAS ASSINATURAS

Código para verificação: 0592-B943-6CA5-7841

Este documento foi assinado digitalmente pelos seguintes signatários nas datas indicadas:

MARICELIA DOS SANTOS (CPF 153.XXX.XXX-10) em 08/12/2023 10:33:11 (GMT-03:00)
Papel: Assinante
Emitido por: Sub-Autoridade Certificadora 1Doc (Assinatura 1Doc)

LUIZ CARLOS ALVES DIAS (CPF 179.XXX.XXX-51) em 08/12/2023 10:39:48 (GMT-03:00)
Papel: Assinante
Emitido por: Sub-Autoridade Certificadora 1Doc (Assinatura 1Doc)

Para verificar a validade das assinaturas, acesse a Central de Verificação por meio do link:

https://cmsantaisabel.1doc.com.br/verificacao/0592-B943-6CA5-7841