POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

ASSOCIAÇÃO DOS MUNICÍPIOS DO MEIO OESTE CATARINENSE - AMMOC

2025

Histórico de versões

Data	Versão	Descrição	Autor
18/08/2025	1.0	Política de Segurança da Informação	Consultora

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

1. Introdução

A **Política de Segurança da Informação (PSI)** é um normativo institucional que tem o papel de estabelecer regras, diretrizes e práticas para a segurança da informação na **ASSOCIAÇÃO DOS MUNICÍPIOS DO MEIO OESTE CATARINENSE - AMMOC,** pessoa jurídica de direito privado, sem fins lucrativos, inscrita no CNPJ nº **82.780.008/0001-82** e sede na Rua Roberto Trompowski 68, 2 Andar, Centro, no município de Joaçaba – SC, CEP 89600-000. Visa a garantir a confidencialidade, integridade e disponibilidade da informação, assegurando seu uso adequado e a mitigação de riscos à segurança da informação. Estipular papéis e responsabilidades claras e objetivas, definir diretrizes de segurança e estabelecer meios de monitoramento do cumprimento da política são processos muito importantes para garantir a segurança da informação. O documento foi elaborado em conformidade com a legislação vigente, em especial com a Lei nº 12.527/2011 (Lei de Acesso à Informação - LAI), Lei nº 12.965/2014 (Marco Civil da Internet), e com a Lei nº 13.709/18 (Lei Geral de Proteção de Dados Pessoais).

2. Propósito

Esta Política de Segurança da Informação tem como objetivo estabelecer os princípios, diretrizes, responsabilidades e práticas para a proteção das informações da AMMOC. A Política visa garantir **a confidencialidade, integridade e disponibilidade** das informações, assegurando o seu uso adequado e a mitigação de riscos à segurança da informação, bem como o cumprimento da Lei nº 13.709/18, Lei Geral de Proteção de Dados Pessoais (LGPD) e de outras normas vigentes.

3. Escopo

Instituir a Política de Segurança da Informação (PSI), no âmbito da AMMOC, com a finalidade de estabelecer princípios e diretrizes para a implementação de ações e controles que garantam a segurança das informações e de dados pessoais, e no que couber, no relacionamento com outras entidades públicas ou privadas.

Esta Política se aplica a todos os ativos de informação da AMMOC, incluindo dados, sistemas, aplicativos, dispositivos e redes. A Política se aplica a todos os agentes políticos, servidores, empregados, comissionados, contratados, parceiros e terceiros que acessam ou processam as informações da entidade.

4. Definição de termos

São conceitos importantes para compreensão dessa Política:

AGENTES DE TRATAMENTO - o controlador ou o operador.
AMEAÇA - conjunto de fatores externos com o potencial de causar em dano para um sistema ou organização.
ANONIMIZAÇÃO - utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo.
ANPD - sigla de Autoridade Nacional de Proteção de Dados.
APLICATIVO - Tipo de programa de computador desenvolvido para processar dados de modo eletrônico, de forma a facilitar e reduzir o tempo do usuário ao executar uma tarefa.
AUTENTICAÇÃO DE DOIS FATORES (2 FACTOR AUTHENTICATION) - processo de segurança que exige que os usuários forneçam dois meios de identificação antes de acessarem suas contas.
BACKUP- conjunto de procedimentos que permitem salvaguardar os dados de um sistema computacional, garantindo guarda, proteção e recuperação. Tem a fidelidade ao original assegurada. Esse termo também é utilizado para identificar a mídia em que a cópia é realizada.
BANCO DE DADOS - coleção de dados inter-relacionados, representando informações sobre um domínio específico. São coleções organizadas de dados que se relacionam, a fim de criar algum sentido (informação) e de dar mais eficiência durante uma consulta ou a geração de informações ou conhecimento.
CONTROLADOR DE DADOS: AMMOC
CONTROLE DE ACESSO - conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso ao uso de recursos físicos ou computacionais. Via de regra, requer procedimentos de autenticação.
DADO PESSOAL: É uma informação relacionada a uma pessoa física e que seja capaz de identificar a pessoa ou tornar possível a sua identificação. São exemplos de dados pessoais que podem permitir a sua identificação: Nome, CPF, telefone, e-mail, placa do seu veículo etc.
DADO PESSOAL SENSÍVEL: Categoria especial de dados pessoais referentes a origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de carácter religioso, filosófico ou político, referentes à saúde ou à vida sexual, dados genéticos ou biométricos relativos a pessoa natural.
DESCARTE - eliminação correta de informações, documentos, mídias e acervos digitais.
DISPONIBILIDADE: propriedade pela qual se assegura que a informação esteja acessível e utilizável, sob demanda, por uma pessoa física ou determinado sistema, órgão ou entidade devidamente autorizados.
DISPOSITIVOS MÓVEIS - equipamentos portáteis, dotados de capacidade de processamento, ou dispositivos removíveis de memória para armazenamento, entre os quais se incluem, não limitando a estes: e-books, notebooks, netbooks, smartphones, tablets, pendrives, USB drives, HD externo, e cartões de memória.
FIREWALL- ferramenta para evitar acesso não autorizado, tanto na origem quanto no destino, a uma ou mais redes. Podem ser implementados por meio de hardware ou software, ou por meio de ambos. Cada mensagem que entra ou sai da rede passa pelo firewall, que a examina a fim de determinar se atende ou não os critérios de segurança especificados.

HACKER – Quem invade sistemas computacionais ou computadores para acessar informações confidenciais ou não autorizadas, apontando possíveis falhas nesses sistemas.
INCIDENTE - interrupção não planejada ou redução da qualidade de um serviço, ou seja, ocorrência, ação ou omissão, que tenha permitido, ou possa vir a permitir, acesso não autorizado, interrupção ou mudança nas operações (inclusive pela tomada de controle), destruição, dano, deleção ou mudança da informação protegida, remoção ou limitação de uso da informação protegida ou ainda a apropriação, disseminação e publicação indevida de informação protegida de algum ativo de informação crítico ou de alguma atividade crítica por um período de tempo inferior ao tempo objetivo de recuperação.
INFORMAÇÃO- dados, processados ou não, que podem ser utilizados para produção e para transmissão de conhecimento, contidos em qualquer meio, suporte ou formato.
INTEGRIDADE- propriedade pela qual se assegura que a informação não foi modificada ou destruída de maneira não autorizada ou acidental.
MALWARE- software malicioso, projetado para infiltrar um sistema computacional, com a intenção de roubar dados ou danificar aplicativos ou o sistema operacional. Esse tipo de software costuma entrar em uma rede por meio de diversas atividades aprovadas pela AMMOC, como e-mail ou sites.
OPERADOR - pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.
PLANO DE GESTÃO E RESPOSTA DE INCIDENTES - plano de ação claramente definido e documentado, para ser usado em caso de incidente que basicamente englobe os principais recursos, serviços e outras ações que sejam necessárias para implementar o processo de gerenciamento de incidentes;
SEGURANÇA DA INFORMAÇÃO- ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações.
TITULAR- É você, a pessoa física a quem os Dados Pessoais se referem.
TRATAMENTO- É toda forma de uso que podemos fazer dos seus Dados Pessoais, incluindo, mas não se limitando às seguintes atividades: coleta, armazenamento, consulta, uso, compartilhamento, transmissão, classificação, reprodução, exclusão e avaliação. Este termo (e outros derivadas dele) não serão utilizados com letras maiúsculas neste documento.
VAZAMENTO DE DADOS - transmissão não autorizada de dados de dentro de uma organização para um destino ou recipiente externo. O termo pode ser usado para descrever dados que são transferidos eletronicamente ou fisicamente. Pode ocorrer de forma acidental ou intencional (pela ação de agentes internos, pela ação de agentes externos ou pelo uso de software malicioso).

5. Condições de Instalação (Equipamentos E Programas)

Todos os equipamentos (computadores, tablets e celulares) utilizados pelos empregados são disponibilizados pela AMMOC e ficam na AMMOC. Ficam os empregados somente autorizados a instalação de programas e aplicativos necessários ao exercício da atividade, gratuitos ou licenciados.

Em caso de utilização de equipamentos pessoais, o empregado se compromete a não armazenar ou compartilhar dados da AMMOC a que tenha acesso em razão da atividade. A AMMOC adota o uso de mensagens instantâneas para comunicação, em especial o Whatsapp, cuja política de uso deve ser cumprida pelos empregados.

6. Gestão de Acessos

O acesso aos sistemas e e-mail é configurado a partir da contratação e bloqueado, mediante informação de desligamento do empregado. O acesso remoto não é realizado pelos empregados.

7. Mecanismos de Proteção

A AMMOC tem sua estrutura de segurança estabelecida por:

a) Atribuir contas e senhas identificáveis a pessoa física para uso de computadores, sistemas, bases de dados e qualquer outro ativo de informação;
b) Ter a instalação antivírus e outras práticas de segurança ao sistema computacional da AMMOC;
c) Estabelecer uma política de backup, com armazenamento em servidor físico;
d) Orientar a definição de senhas individuais, não disponibilizados ou anotadas, e compostas por letras, números e caracteres especiais;
e) Utilizar o e-mail e whatsapp da AMMOC somente para atividades profissionais, não acessando e-mails suspeitos ou compartilhando e-mails ou informações sigilosas ou que comprometam a AMMOC;
f) Utilizar a internet para atividades profissionais relacionadas à AMMOC, sem baixar arquivos ou programas não autorizados;
g) gestão de contratos com fornecedores.

8. Responsabilidade dos Colaboradores

São responsabilidades exigidas pelos empregados da AMMOC:

a) Respeitar esta Política de Segurança da Informação e demais políticas afetas à segurança de dados e normas de conduta;

b) Realizar a guarda e proteção dos recursos computacionais disponibilizados para o trabalho;
c) Responder pelo uso exclusivo e intransferível de suas senhas de acesso;
d) Realizar a correta utilização dos recursos de hardware e software;
e) Relatar prontamente qualquer fato ou ameaça à segurança dos recursos, como quebra da segurança, fragilidade, mau funcionamento, presença de vírus, etc;
f) Assegurar que as informações e dados de propriedade da AMMOC não sejam disponibilizados a terceiros, a não ser com autorização por escrito do responsável hierárquico;
g) Relatar para o seu responsável hierárquico o surgimento da necessidade de um novo software para suas atividades.
h) Responder pelo prejuízo ou dano que vier a provocar a AMMOC ou a terceiros, em decorrência da não obediência às diretrizes e normas aqui referidas.

Em caso de dúvidas, comentários e/ou sugestões relacionadas a esta Política, entre em contato nos seguintes endereços de contato: Encarregado de Dados: Lauri Nora: encarregadodedados@ammoc.org.br e telefone: (49) 3522 2800.

Aprovado em setembro de 2025.

Presidente da AMMOC