CARTILHA DE SEGURANÇA DA INFORMAÇÃO

CAAPSML

Elaborada pela Comissão de Segurança da Informação da CAAPSML, instituída pela Portaria nº 105/2026.

“Segurança da Informação começa com você.”

Esta cartilha foi elaborada integrando as diretrizes da Política de Segurança da Informação (PSI) da CAAPSML com as melhores práticas de segurança digital.

🔒 REGRAS DE OURO DA SEGURANÇA DA INFORMAÇÃO

1. **Proteja suas senhas – Nunca compartilhe**
2. **Desconfie de e-mails – Não clique sem verificar**
3. **Mantenha tudo atualizado – Sistema e antivírus**
4. **Use apenas sistemas oficiais**
5. **Evite armazenar dados em locais indevidos**
6. **Comunique incidentes imediatamente**

CONTEXTUALIZAÇÃO

Considerando a crescente utilização de dispositivos móveis e estações de trabalho no desempenho das atividades institucionais da CAAPSML, bem como a consequente exposição a riscos, fragilidades e vulnerabilidades no ambiente digital, torna-se imprescindível o fortalecimento de uma cultura organizacional voltada à segurança da informação.

Assim, a adoção de boas práticas e o adequado uso dos recursos tecnológicos são medidas essenciais para a mitigação de riscos, a proteção de dados institucionais e pessoais, e a garantia da continuidade e confiabilidade dos serviços prestados pela Autarquia.

Assim, a presente cartilha tem por finalidade promover a conscientização dos(as) servidores(as) ativos, aposentados e pensionistas, colaboradores(as) e prestadores(as) de serviço quanto ao uso seguro dos recursos tecnológicos, contribuindo para a prevenção de incidentes de segurança da informação no âmbito da CAAPSML.

OBJETIVOS DA CARTILHA

- Apresentar conceitos fundamentais relacionados à segurança da informação e sua relevância no contexto institucional;
- Orientar quanto às principais ameaças existentes no ambiente virtual e seus potenciais impactos;
- Indicar boas práticas de segurança da informação, visando à prevenção, mitigação e redução de danos decorrentes de incidentes;
- Promover o uso seguro dos sistemas institucionais, em especial do Sistema Eletrônico de Informações (SEI!) e demais ferramentas adotadas pela CAAPSML.

Ressalta-se que a efetividade das medidas de segurança da informação depende, em grande parte, do comportamento dos usuários. Estudos indicam que aproximadamente 95% dos incidentes de segurança cibernética decorrem de falhas humanas, o que reforça a importância da conscientização contínua e da adoção de condutas seguras no ambiente digital.

ESCOPO DA CARTILHA

A presente cartilha insere-se no conjunto de ações voltadas ao fortalecimento da cultura de Segurança da Informação no âmbito da CAAPSML, em consonância com as diretrizes estabelecidas em sua Política de Segurança da Informação e com as boas práticas amplamente reconhecidas em âmbito nacional e internacional.

Nesse contexto, destaca-se que a promoção da educação e da conscientização dos usuários constitui elemento essencial para a prevenção de incidentes e para a adequada proteção dos ativos de informação da Autarquia. Assim, a disseminação de conhecimento e a adoção de práticas seguras no uso dos recursos tecnológicos são pilares fundamentais para a mitigação de riscos cibernéticos.

Dessa forma, esta cartilha tem como escopo disponibilizar conteúdo didático, objetivo e acessível, contemplando orientações práticas de segurança da informação, com foco no uso adequado dos sistemas institucionais, dos dispositivos tecnológicos e no tratamento responsável das informações no âmbito da CAAPSML.

Adicionalmente, busca-se fomentar a mudança de comportamento dos usuários, promovendo maior responsabilidade no uso dos recursos digitais e contribuindo para o fortalecimento contínuo da cultura de segurança da informação na Autarquia.

BOAS PRÁTICAS DE SEGURANÇA DA INFORMAÇÃO

Realização de Backup

O backup consiste na criação de cópias de segurança das informações, sendo medida essencial para garantir a disponibilidade e a integridade dos dados institucionais da CAAPSML.

A perda de dados pode ocorrer em razão de falhas de hardware, erros operacionais, ataques cibernéticos, extravio de dispositivos ou corrupção de arquivos. Nesse contexto, a realização periódica de backups é indispensável para assegurar a continuidade das atividades administrativas.

Diretrizes:

- Realizar backups periódicos dos arquivos de trabalho, conforme orientações da área de TI;
- Priorizar o armazenamento em ambientes institucionais seguros;
- Evitar manter arquivos exclusivamente em dispositivos locais;
- Verificar regularmente a integridade e possibilidade de restauração dos backups.

Observações:

- Serviços de armazenamento em nuvem (ex.: Google Drive, OneDrive) realizam sincronização de arquivos, mas não substituem integralmente políticas estruturadas de backup;
- Backups institucionais podem incluir cópias em servidores e mídias externas, conforme política interna.

Uso de Dispositivos Móveis (Celulares)

Os dispositivos móveis utilizados para acesso a sistemas institucionais devem ser tratados como ativos de informação sensíveis.

Em caso de perda, furto ou roubo, devem ser adotadas imediatamente as seguintes providências:

- Registrar boletim de ocorrência;
- Solicitar o bloqueio da linha telefônica junto à operadora;
- Solicitar o bloqueio do aparelho (IMEI);

Boas práticas adicionais:

- Utilizar senha, biometria ou reconhecimento facial;
- Manter o sistema operacional atualizado;
- Ativar recursos de localização, bloqueio e limpeza remota do dispositivo;
- Evitar o armazenamento de informações institucionais sensíveis em dispositivos pessoais.

Atenção a Phishing (Fraudes Eletrônicas)

Ataques phishing crescem diariamente e ainda conseguem elevado percentual de êxito. Por isso, a mitigação desse tipo de ataque requer principalmente a percepção do(a) usuário(a) em relação às informações e demandas oriundas de e-mails.

Mas o que é phishing? Trata-se de uma técnica de engenharia social usada para enganar usuários e obter informações confidenciais como nome de usuário, senha e detalhes do cartão de crédito, por exemplo. Para cometer as fraudes eletrônicas, os criminosos utilizam mensagens eletrônicas aparentemente reais, por isso algumas iniciativas mitigam esse tipo de ataque, como as relacionadas a seguir:

Como combater o *phishing?*

- Proteja suas credenciais. Se uma pessoa está pedindo informações confidenciais, não tenha medo de perguntar o porquê; geralmente as empresas não solicitam informações confidenciais por e-mail, mensagem de texto ou telefone;
- Cuidado com anexos e links, pois são comumente usados para enviar software mal-intencionado. Quando você receber uma mensagem com um anexo ou link, verifique sua legitimidade antes de clicar;
- Verifique o endereço de e-mail do remetente antes de responder ou clicar em links. Como os e-mails podem ser falsificados, passe o cursor sobre os endereços antes de responder para garantir que sejam legítimos. Qualquer correspondência de uma organização deve vir de um endereço de e-mail organizacional;
- Limite suas informações públicas. Os invasores usam informações pessoais e públicas sobre você para convencê-lo a responder. Quanto menos você compartilhar sobre si mesmo, menor será o alvo de um ataque de engenharia social. Os criminosos cibernéticos usam as informações que você publica online para saber como ganhar sua confiança;

- Não se pressione. E-mails que criam urgência e medo geralmente são falsos. Não se apresse, olhe todo o e-mail e seja cético(a): verifique novamente o endereço do remetente para ver se é legítimo; e
- Pare e reveja. Olhe o e-mail antes de responder. É inesperado? O pedido faz sentido? Em caso de dúvida, entre em contato com o remetente, separadamente, por telefone ou por e-mail (mas não responda ao e-mail suspeito).

Senhas e Credenciais de Acesso

No âmbito da CAAPSML, o uso de senhas é indispensável para o acesso aos sistemas corporativos, redes e demais ambientes institucionais. A utilização de senhas inadequadas representa um dos principais riscos à segurança da informação, podendo permitir o acesso indevido a dados sensíveis da Autarquia.

Senhas consideradas fracas — como sequências numéricas simples ou palavras comuns (ex.: “123456”, “12345678”, “Brasil”) — podem ser facilmente descobertas por mecanismos automatizados em poucos segundos, comprometendo a confidencialidade, integridade e disponibilidade das informações institucionais.

Com o objetivo de fortalecer a segurança dos acessos, todos os usuários da CAAPSML devem observar as seguintes diretrizes:

- Utilizar senhas fortes, com no mínimo:
  - 8 caracteres (com autenticação em dois fatores – 2FA);
  - 12 a 14 caracteres (sem 2FA);
- Combinar letras maiúsculas, minúsculas, números e símbolos;
- Não reutilizar senhas em diferentes sistemas;
- Alterar senhas periodicamente ou sempre que houver suspeita de comprometimento;
- Não compartilhar senhas sob nenhuma hipótese;
- Não armazenar senhas em locais inseguros (papel, e-mails, arquivos desprotegidos).

Recomendações adicionais:

- Utilizar autenticação em dois fatores (2FA) sempre que disponível;
- Utilizar gerenciadores de senhas confiáveis, quando autorizado;
- Configurar mecanismos de recuperação de acesso.

Acesso a Sites e Conteúdos na Internet

O acesso a sites deve observar critérios de segurança e finalidade institucional.

É vedado:

- Acessar sites com conteúdo ilícito ou incompatível com o ambiente institucional;
- Realizar download de softwares não autorizados;
- Utilizar programas sem licença ou de origem desconhecida.

Recomendações:

- Verificar a reputação de sites antes de acessá-los;
- Priorizar conexões seguras (https);
- Em caso de dúvida, consultar a área de TI.

Uso de Mídias Removíveis (Pendrives, HDs Externos)

O uso de mídias removíveis representa risco relevante de contaminação por malware.

Diretrizes:

- Evitar o uso de dispositivos desconhecidos;
- Realizar verificação antivírus antes de acessar arquivos;
- Utilizar apenas mídias autorizadas, quando necessário;
- Não conectar dispositivos pessoais em equipamentos institucionais sem autorização.

Utilização de Antivírus

A proteção contra softwares maliciosos é requisito básico de segurança.

Boas práticas:

- Manter antivírus instalado e atualizado nos equipamentos;
- Não desativar mecanismos de proteção;
- Realizar verificações periódicas no sistema;
- Evitar instalação de softwares fora dos padrões institucionais.

Uso de Ferramentas de Inteligência Artificial (ex.: ChatGPT)

Ferramentas baseadas em inteligência artificial devem ser utilizadas com cautela no ambiente institucional.

ChatGPT (Chat Generative Pre-Trained Transformer/Transformador Pré-Treinado de Gerador de Conversas) é um assistente virtual inteligente no formato chatbot online com inteligência artificial desenvolvido pela OpenAI, sendo um aplicativo especializado em diálogo. O chatbot é um modelo de linguagem ajustado com técnicas de aprendizado supervisionado e por reforço.

O aplicativo tem sido amplamente utilizado para atender a diversas necessidades, tais como: elaboração de apresentações, artigos, sermões, fórmulas de planilhas eletrônicas, código de programas computacionais, cartas e demais atividades do cotidiano. Porém, como o aplicativo requer massa de informações para seu aprimoramento, o conteúdo inserido em sua plataforma poderá ficar acessível a outros usuários, que terão a possibilidade de usá-lo de forma indevida.

Como evitar ataques cibernéticos propiciados pelas informações no ChatGPT?

Boas práticas de configurações no ChatGPT têm sido disseminadas com o intuito de manter a privacidade das informações. Contudo, como se trata de uma ferramenta relativamente nova, a ameaça está evoluindo rapidamente. Existem algumas maneiras de se proteger contra possíveis ataques:

- Nunca compartilhe informações confidenciais, como dados financeiros, objetivos estratégicos, metas da organização, indicadores, logins/senhas ou

mesmo seu nome e endereço;

- Mantenha-se alerta a ataques de engenharia social;
- Não insira código-fonte no aplicativo;
- Permaneça atualizado com relação aos procedimentos de segurança propostos pela organização.

O uso inadequado dessas ferramentas pode resultar em vazamento de informações e responsabilização administrativa, civil e legal.

Disposição Final

A adoção das boas práticas descritas nesta cartilha é fundamental para a proteção dos ativos de informação da CAAPSML, contribuindo para a conformidade com a LGPD, o fortalecimento dos controles internos e o atendimento aos requisitos do Pró-Gestão RPPS e dos órgãos de controle.

Este material deve ser revisado periodicamente para garantir aderência às normas vigentes, evolução tecnológica e requisitos dos órgãos de controle.