

Prefeitura Municipal de Maricá

Instituto de Ciência, Tecnologia e Inovação de Maricá



Anexo II - Norma para Uso de Equipamentos e Softwares

Maricá, abril de 2025

Presidente

Cláudio de Souza Gimenez

Diretor de Infraestrutura

Laércio Aguiar da Rocha

Equipe Técnica

Emerson Lacerda Alencar

Giovanni Di Carlo

Márcio Santarém Nogueira

Histórico de Revisões

Versão	Data	Histórico	Autor	Revisor
1.0	abril de 2025	Versão inicial	Emerson L. Alencar Márcio S. Nogueira	Laércio A. Rocha

Sumário

1.	PREMISSAS.....	4
2.	CONCEITOS.....	4
3.	DIRETRIZES	4

1. PREMISSAS

- 1.1. É fundamental que todos os servidores públicos, diretorias, fornecedores, prestadores de serviços e demais parceiros vinculados compreendam o seu papel crucial no contexto da Segurança da Informação (SI). É um dever seguir rigorosamente as diretrizes e orientações estabelecidas na Política de Segurança da Informação (PSI) do ICTIM, a fim de evitar exposição indevida das informações e dos recursos de processamento a situações adversas, tais como comprometimento, alteração, furto e desvio.

2. CONCEITOS

- 2.1. Computadores, sistemas e serviços conectados à rede corporativa do ICTIM devem estar em conformidade com a Norma para Padrões de Segurança da Informação, conforme as competências nela estabelecidas, proporcionando assim um ambiente seguro e eficiente para os usuários.
- 2.2. A **responsabilidade pela Segurança da Informação** não recai apenas sobre a Assessoria de TI ou a Gestão do ICTIM, mas é **compartilhada** por todos os que **utilizam** a informação, seja em meio digital ou físico.
- 2.3. A adoção de **boas práticas no uso diário** de hardware e software contribui significativamente para a melhoria geral da TI e, em particular, para a Segurança da Informação.
- 2.4. É **responsabilidade do usuário** estar ciente destes conceitos e seguir as diretrizes deste documento, bem como as orientações do Guia de Boas Práticas de Segurança da Informação.

3. DIRETRIZES

DE SOFTWARE

- 3.1. **Não é permitido propagar** qualquer tipo de códigos maliciosos (malwares), spam, mineradores, crackers, keyloggers, sniffers, propagandas de qualquer tipo ou programas de controle remoto de outros computadores, utilizando a rede, os computadores e a internet disponibilizados pelo ICTIM.
- 3.2. **Fica vedada e caracterizada como ato grave**, toda ação que possa ferir a propriedade intelectual de software (Lei 9.609/98 - Proteção da propriedade intelectual de programa de computador), como o uso de geradores de chaves de registro, crackers de senhas e/ou engenharia reversa de qualquer natureza.

- 3.3. É **proibida a instalação de qualquer** software nos computadores pelos **usuários**, mesmo sendo software livre, shareware ou freeware. Qualquer instalação de software **deverá** ser feita somente pela equipe de TI responsável.
- 3.4. **Não é permitido copiar** nenhum software ou informações de qualquer tipo, de propriedade de qualquer órgão municipal, por qualquer meio existente, bem como licenças de uso de software pertencentes a estes, instaladas em computadores pertencentes ao ICTIM.
- 3.5. Materiais de **cunho sexual** ou de **condutas ilícitas não poderão** ser expostos, armazenados, distribuídos, editados, impressos ou gravados por meio de qualquer recurso disponibilizado pelo ICTIM.

USO DE EQUIPAMENTOS DE INFORMÁTICA

- 3.6. É de **responsabilidade do usuário** zelar pela integridade física dos equipamentos de informática colocados à sua disposição, mantendo-os limpos e em boas condições.
- 3.7. **Não é permitido** colar adesivos ou fotos nos equipamentos de informática disponibilizados pelo ICTIM, bem como riscar, raspar ou retirar a etiqueta de patrimônio ou de licenças de software.
- 3.8. **Não é permitido aos usuários**, abrirem os equipamentos de informática para reparo ou qualquer outro motivo. Caso seja necessário, a abertura/reparo deverá ser feita somente pela equipe de TI responsável ou empresa contratada para este fim.
- 3.9. **Todos os computadores e dispositivos** devem ser desligados ou ter seu uso bloqueado (via função “bloquear/lock” do sistema operacional) ao final do expediente. Durante o expediente, caso o usuário se ausente, deverá bloquear o computador (via função “bloquear/lock” do sistema operacional).
- 3.10. Cabe apenas à equipe de TI pela **responsabilidade de instalação, manutenção e substituição** de equipamentos de rede, sendo proibido aos demais usuários conectarem equipamentos à rede física ou Wi-Fi do ICTIM, quais sejam roteadores, switches, modems ou similares.
- 3.11. A **conexão de equipamentos na rede elétrica**, onde estão ligados os computadores e impressoras, está limitada aos equipamentos homologados e autorizados pelo ICTIM. Em caso de dúvidas e eventuais necessidades deve-se verificar junto à Diretoria de Infraestrutura.

USO DE IMPRESSORAS

- 3.12. As impressoras são ferramentas para **fins de trabalho**, não sendo permitidas **impressões para fins pessoais**.
- 3.13. Este equipamento deve ser utilizado apenas quando o documento físico se fizer **imprescindível**, evitando impressão de **dados sensíveis, desperdícios e gastos desnecessários**.
- 3.14. **Não é permitido deixar nas impressoras**, impressos com dados pessoais, informações consideradas sensíveis pela Lei Geral de Proteção de Dados Pessoais - LGPD, Lei Federal nº 13.709/2018 e demais informações que não tenham classificação pública.
- 3.15. Na eventualidade de trato de informações referenciadas na Lei 12.527 (LAI) como Secretas ou Ultrassecetas, essas **não podem ser impressas** via recursos de rede, devendo ser impressas em impressoras **diretamente ligadas ao equipamento**.