

## Política de Utilização Aceitável Tecnologias de Informação

### A. Objeto e âmbito de aplicação

1. Estas políticas foram emitidas pela Conselho de Administração da Maiêutica em complacência com seus princípios e missão, tornando-se obrigatória para todos os docentes, estudantes, investigadores, colaboradores ou terceiros, devidamente autorizados que acedam a qualquer sistema informático, equipamento isolado ou dispositivo móvel, pertença ou meramente operado pela Maiêutica desde que propriedade da Maiêutica.

2. Em conformidade com o ponto anterior, estas políticas estendem-se também aos equipamentos usados no exterior ao campus universitário.

3. O propósito destas políticas, é proteger os ativos de informação detidos e utilizados pela Maiêutica, de todas as ameaças quer internas ou externas, deliberadas ou acidentais e satisfazer todas as exigências regulamentadas e/ou legisladas.

### B. Direitos de Autor

1. A proteção conferida pelos Direitos de Autor é reconhecida em todos os países da União Europeia, nos países subscritores da Convenção de Berna para a Proteção de Obras Literárias e Artísticas e nos países membros do Tratado OMPI (Organização Mundial da Propriedade Intelectual).

2. Livros, periódicos, imagens, fotografias, gravações áudio, são exemplos de materiais ou trabalhos que podem estar protegidos por Direitos de Autor.

3. Se for necessário publicar ou descarregar conteúdos de websites como parte de uma função ou atividade regular da instituição, o(s) envolvido(s) são responsáveis por garantirem que os Direitos de Autor não sejam violados.

4. A partilha de arquivos ponto a ponto (p2p) geralmente envolve conteúdos protegidos.

5. Todos os computadores da Instituição são auditados regularmente como parte das condições de alcançar e manter o credenciamento da Instituição perante as entidades que zelam pelos Direitos de Autor.

### C. Software

#### Licenciamento

1. A legislação dos Direitos de Autor que regulamenta o uso de propriedade intelectual incluindo o software, é muito clara - é ilegal copiar qualquer peça de software a menos que expressamente permitido pelo legal detentor dos direitos.

2. Se forem utilizadas cópias ilegais de software, a Instituição não só pode enfrentar um processo-crime seguido de um cível, mas também podem ser arrolados nestes processos os diretores da Instituição e os utilizadores que individualmente ou em coletivo tiveram ação significativa no processo, respondendo solidariamente perante responsabilidade criminal e cível.

3. Caso seja feita uma associação Maiêutica a praticas violadoras da propriedade intelectual, o dano potencial para o nome bom da Instituição é imensurável.

#### Utilização

4. Os Serviços de Informática poderão disponibilizar aos colaboradores software pertença da Instituição ou disponibilizar os respetivos media ou instaladores, somente no âmbito do regime de licenciamento em vigor para cada software e caso seja demonstrada sua necessidade.

5. É interdito a qualquer colaborador da Instituição efetuar cópias ou proporcionar o acesso a software pertença da Maiêutica a estranhos, inclusive a estudantes e docentes, excetuando os casos referidos no ponto anterior.

6. Qualquer utilizador que reproduza software de forma ilegal, ficará sujeito às penalidades criminais e cíveis que daí possam advir, sem prejuízo da responsabilidade disciplinar perante a Instituição.

7. Todo o software deve ser adquirido por recomendação dos Serviços de Informática, que instalarão as licenças e respetivo software nos computadores ou servidores designados.

8. Os Serviços de Informática informarão todas as condições aplicáveis ao licenciamento do software em uso pelos utilizadores caso seja solicitado.

### **Instalação**

9. A instalação ou execução de jogos, proteções de ecrã ou programas lúdicos em geral, não é permitida em qualquer computador da Instituição, salvo com autorização expressa dos Serviços de Informática.

10. Em caso de necessidade de software, o colaborador deverá formalizar um pedido ao seu superior hierárquico. Relativamente aos laboratórios de informática, é enviado semestralmente um e-mail a todos os coordenadores de curso, com um formulário para registo das necessidades ao nível do software e licenças.

11. O uso de software freeware ou shareware só deverá ser permitido para propósitos do negócio da Instituição, tendo em conta que é autorizado e providenciada a sua instalação pelos Serviços de Informática.

### **D. Infraestrutura tecnológica**

1. A Instituição tem procedimentos para lidar com as ameaças de vírus, software malicioso, risco de roubo de hardware e software, bem como acesso não autorizado a dados informatizados pelos utilizadores.

2. Os administradores de sistemas dos Serviços de Informática, têm autoridade para encerrar imediatamente qualquer programa ou acesso suspeito que possa prejudicar as operações normais.

3. Os utilizadores não podem revelar qualquer informação relativa às facilidades das tecnologias de informação da Instituição perante qualquer pessoa ou entidade externa à Maiaútica, sem a permissão expressa do Conselho de Administração. Qualquer pedido neste sentido deverá ser dirigido diretamente para a direção dos Serviços de Informática.

### **Armazenamento de informação**

4. Os utilizadores deverão guardar toda a informação relevante na área pessoal de rede, ou noutras áreas criadas para o efeito, e devidamente identificadas. A Maiaútica não se responsabiliza pela perda de informação alojada em dispositivos amovíveis como por exemplo *pen drives*. É fundamental que os utilizadores efetuem cópias de segurança dos conteúdos dos dispositivos amovíveis para a rede periodicamente.

### **Registos de acessos**

5. Existem métodos de identificação e localização dos equipamentos de rede, sendo recolhidos registos relativos à utilização dos sistemas informáticos, nomeadamente endereços IP, portos, protocolos, data, hora, browser e metadados relacionados com as camadas 3 e 4 do modelo Open System Interconnection (OSI).

6. Na ausência de outro prazo de conservação dos registos definido nas condições de utilização particulares do serviço ou por imposição legal, os registos serão mantidos por um período máximo de 24 meses.

### **Contas de utilizador**

7. É fornecido a todos os utilizadores um nome de utilizador (login) e uma senha (password) que são únicos e nunca deverão ser partilhados com outras pessoas em nenhuma circunstância.

8. A senha da conta institucional de docente, aluno ou colaborador, deverá ser sempre diferente das utilizadas no registo de sites online ou serviços pessoais;

a. Não devem ser escritas ou deixadas onde terceiros as possam encontrar.

b. Devem ser difíceis de adivinhar e conter nove caracteres no mínimo, incluindo pelo menos uma maiúscula, uma minúscula, um número e caracteres especiais tais como ! # £ \$.

c. Devem ser alteradas a intervalos regulares de tempo.

d. Os utilizadores da rede pedagógica (alunos, docentes, bolsеiros, investigadores) podem alterar sua password através da sua área privada do portal da instituição ou dirigindo-se aos Serviços de Informática. No caso da rede administrativa, a alteração é efetuada no próprio posto de trabalho, através da combinação das teclas CTRL+ALT+DEL.

## Acessos

13. O utilizador nunca deverá deixar o computador com a sessão aberta sem bloquear antes a respetiva consola.
14. A Maiêutica responsabiliza criminal e civilmente qualquer tentativa deliberada de acesso a um sistema informático, seja software ou hardware, para o qual não tenha autorização.
15. Os equipamentos portáteis propriedade da Maiêutica nunca deverão ficar desacompanhados em qualquer local, nem serem deixados à vista dentro de viaturas, transportes públicos e de uma forma geral em qualquer local que não ofereça condições de segurança.
16. Nenhum dispositivo ou periférico de qualquer tipo (máquinas fotográficas digitais, dispositivos móveis, etc.) pode ser instalado ou configurado nos computadores da Instituição, exceto com autorização expressa e apoio dos Serviços de Informática.
17. É proibida a utilização de equipamentos portáteis pessoais na área administrativa, com ligações wireless ou por cabo, sem autorização prévia da direção dos Serviços de Informática.

## Redes Virtuais Privadas (VPN)

18. Todos os utilizadores com autorização para o uso de Redes Virtuais Privadas (VPN), deverão ter sempre o seu computador, portátil ou dispositivo móvel protegido com antivírus atualizado e todas as atualizações de segurança do sistema operativo.

## Manuseamento de equipamento

19. A remoção ou destruição de equipamento informático é efetuada pelos Serviços de Informática após coordenação com o Departamento Financeiro e Centro de Apoio Técnico à Segurança no Trabalho. Este processo é efetuado de acordo com as leis ambientais, assegurando que são atualizados os registos de hardware e software internos.
20. Somente aos membros da equipa dos Serviços de Informática é permitido alterar de local equipamento informático.
21. Cada utilizador deve usar o equipamento de forma segura, responsável e apenas para o fim pretendido. Todos os equipamentos devem ser mantidos limpos e em boas condições de utilização, mantendo alimentos e bebidas afastados dos equipamentos.

## E. Correio Eletrónico

1. A Maiêutica providencia o uso de plataformas colaborativas e correio eletrónico para apoio à comunicação entre todos os utilizadores e o seu uso deverá ser limitado às atividades oficiais da Instituição.
2. Porém, o uso pessoal, acidental e ocasional do correio eletrónico é permitido, com a compreensão que as mensagens pessoais poderão ser tratadas como as mensagens organizacionais.
3. O uso pessoal do sistema de correio eletrónico nunca deverá afetar o fluxo de tráfego normal do correio a nível organizacional.
4. O utilizador deve utilizar o correio eletrónico de forma segura, produtiva, profissional e verificar sempre os endereços dos destinatários.
5. Não deve subscrever listas de correio eletrónico que não sejam realmente úteis. Os volumes de mensagens que podem ser geradas são elevados e não existe nenhum controlo sobre o seu conteúdo.

## Conteúdos

6. Nenhuma mensagem deverá ser enviada ou recebida com conteúdo relacionado com atividades ilegais ou para benefícios financeiros pessoais.
7. Nenhum utilizador deve usar o sistema de correio eletrónico com conteúdo que possa ser interpretado como insulto, ou seja ofensivo por qualquer outra pessoa, ou empresa, ou sob qualquer forma que possa ser prejudicial para a imagem Institucional.
8. Exemplos de material proibido incluem: mensagens sexualmente explícitas, caricaturas, anedotas, pedidos para encontros, ou cartas de amor; profanação, obscenidade, difamação, calúnia, discriminação étnica, discriminação religiosa, ou discriminação racial; manifestações de convicções políticas ou comentários, ou qualquer outra mensagem que possa ser interpretada como assédio sexual ou depreciação de outros baseado no sexo, cor, orientação sexual, idade, origem nacional, inaptidão, ou convicções religiosas ou políticas.

9. Não devem ser efetuados compromissos contratuais por correio eletrónico a não ser como precursores de uma carta formal ou contrato escrito.

### Spam

10. O envio de mensagens para cadeias, seja de solidariedade ou não, é proibido. Isto inclui aquelas que pretendendo ser para caridade ou outras boas causas como também para concursos ou outros ganhos pessoais. Também se incluem aqui advertências sobre vírus; a maioria destas mensagens é falsa. Quem desejar conferir a veracidade destas mensagens deve contactar os Serviços de Informática, mas não deve remeter as mensagens, de forma alguma, para qualquer pessoa dentro ou fora da Instituição, nem clicar em links que não ofereçam confiança.

11. Não deverá ser enviada nenhuma mensagem de qualquer tipo para múltiplos recipientes sem fundamento. Isto pode ser considerado como “spam” e é considerada uma atividade ilegal em muitos países.

### Segurança das comunicações

12. Para todas as mensagens, deverá ser tido em atenção que o correio eletrónico não é uma forma segura de comunicação. As mensagens que são enviadas passam por servidores e redes propriedade de outras entidades. O conteúdo da mensagem pode causar problemas para a imagem, ou perdas financeiras, à Maiêutica caso seu conteúdo se torne público. Nestes casos, um método de comunicação mais seguro deve ser usado. Para tal, devem ser contactados os Serviços de Informática para que seja providenciado um método com encriptação de dados nas mensagens de correio eletrónico a enviar.

13. O utilizador que se autenticou num computador será considerado o autor de qualquer mensagem enviada desse computador. É aconselhado bloquear a consola ou encerrar a sessão do computador quando se ausente do seu posto de trabalho. De modo algum devem ser enviados e-mails de um computador onde não foi efetuado o início de sessão com o próprio nome de utilizador.

14. Os endereços de correio eletrónico não devem ser públicos sem justificação. Ao ser colocado o endereço de e-mail ao preencher pesquisas ou outros questionários, existe o risco de receção de correio não solicitado.

### Anexos

15. O correio eletrónico não deve ser usado para o envio de grandes arquivos apensos, a menos que seja indispensável. Muitos sistemas de correio eletrónico não aceitam grandes arquivos, sendo os mesmos devolvidos e podendo resultar em sobrecarga do próprio sistema de correio eletrónico. Para enviar grandes arquivos, deverão ser usados dispositivos amovíveis, Microsoft OneDrive Institucional, ou pedir auxílio aos Serviços de Informática.

16. Não devem ser abertos anexos de correio eletrónico (executáveis essencialmente) a menos que sejam esperados. Caso seja inevitável a abertura, deverá ser efetuada com extrema precaução.

### Phishing

17. Nunca nenhum utilizador poderá clicar em hiperligações de mensagens de correio eletrónico suspeitas e que não tenham sido solicitadas. Tentativas de phishing podem surgir através de websites ou e-mails falsos, que passam a imagem de uma empresa conhecida e confiável para poderem chamar a atenção dos destinatários. Normalmente, os conteúdos dos sites ou e-mails phishing prometem por exemplo, promoções extravagantes para o utilizador ou solicitam que faça uma atualização dos seus dados bancários, evitando o cancelamento da conta.

### Endereços de e-mail pessoais

18. A facilidade de envio de e-mails por contas pessoais existe, mas não deverá ser utilizada. Os Serviços de Informática preveem soluções para permitir o acesso ao correio eletrónico institucional fora do campus universitário.

## F. Acesso Internet

1. A Maiêutica disponibiliza acesso à Internet a todos os utilizadores autenticados. Onde este acesso é fornecido, subentende-se que a sua utilização deverá ser limitada à atividade oficial da Instituição em ambiente académico ou administrativo. Porém, é admitida a possibilidade de utilização da internet para fins pessoais

2. O acesso não poderá ser utilizado para ganhos financeiros pessoais, venda de serviços ou produtos, nem para alojamento de websites.

### Publicação de conteúdos

3. Nenhum conteúdo ou mensagem que possa comprometer ou criar conflitos à Instituição, por serem ofensivos ou abusivos, poderá ser colocada na Internet. Material proibido ou protegido por direito de autor está em igual circunstância, bem como o envolvimento em atividades ilegais enquanto usa o acesso Internet.

### Navegação

4. Deve evitar a visita a sites que exibam conteúdos de natureza pornográfica, ou que contenham material que possa ser considerado ofensivo ou ilícito, salvo que seja importante para fins académicos. Sempre que um utilizador for surpreendido, acidentalmente, com páginas web de conteúdos suspeitos, deve informar de imediato os Serviços de Informática.

5. É expressamente proibido:

- a. O acesso a servidores sem autorização.
- b. Detecção de serviços em servidores ("Port Scan").
- c. Alteração de endereços IP (IP Spoofing).
- d. A utilização de softwares peer-to-peer (P2P), como por exemplo: Kazaa, BitTorrent, Emule, etc.

6. O utilizador deve estar atento aos Direitos de Autor dos conteúdos que descarregar da Internet.

7. Nunca deverá o utilizador indicar o seu endereço de correio eletrónico desnecessariamente num website. Ao fornecer o seu endereço preenchendo pesquisas ou outros questionários está a correr o risco de receber mensagens impróprias que não têm qualquer interesse.

### Partilha de computadores

8. O utilizador com sessão ativa no computador será considerado como a pessoa que está a aceder à Internet. De modo algum deverá utilizar a Internet através de um computador com a sessão de utilizador de outra pessoa.

### Incidentes de segurança

9. Em caso de incidente de segurança ou deteção de vulnerabilidades, deverão ser informados de imediato os Serviços de Informática através do endereço de e-mail [incidente.seguranca@maieutica.pt](mailto:incidente.seguranca@maieutica.pt), para que possam ser efetuadas as diligências mais adequadas, em conformidade com os procedimentos internos. O e-mail enviado, deverá conter informação sobre o computador e sistema operativo afetado, programas utilizados e tipo de incidente.

### G. Responsabilidade e alterações às atuais políticas

1. Qualquer suspeita ou fuga às Políticas de Utilização Aceitável (PUA), que possa afetar os sistemas da organização, será devidamente investigada pelos Serviços de Informática internos ou por terceiros especialmente contratados para o efeito. Poderá ser aplicada uma ação disciplinar que pode em última instância conduzir a inquérito interno, não impedindo, contudo, uma ação criminal.

2. No caso de dúvida ou conhecimento de alguma violação a estas políticas, envie e-mail para [gisi.infra@maieutica.pt](mailto:gisi.infra@maieutica.pt).

3. Qualquer aditamento ou revisão, este documento será atualizado e tornado público nos websites de cada Instituição e em <https://maieutica.pt/aup>.

### Contatos:

Maiêutica - Cooperativa de Ensino Superior, CRL  
Gabinete de Informática e Sistemas de Informação  
Avenida Carlos de Oliveira Campos - Castelo da Maia / 4475-690 Maia  
+351229866044 / extensão: 1030  
[helpdesk@maieutica.pt](mailto:helpdesk@maieutica.pt)