POLÍTICA DE UTILIZAÇÃO ACEITÁVEL DA REDE

AUP (*ACCEPTABLE USE POLICY*)

INTRODUÇÃO

A rede da Escola Superior de Enfermagem de Lisboa interliga os recursos necessários ao funcionamento dos Serviços Tecnológicos. Fornece acesso de conectividade local e com a Internet, permitindo a comunicação de computadores de postos de trabalho, laboratórios e salas de aula, computadores portáteis e *smartphones* pessoais, servidores, terminais telefónicos, equipamentos de impressão e diversos serviços de rede.

Para além dos equipamentos próprios da ESEL, os utilizadores têm acesso a diversos serviços de comunicações para obter ligação à internet. A conectividade local e com a internet, através da RCTS, proporciona vantagens aos utilizadores mas também requer que sejam aceites e cumpridas as responsabilidades pessoais na salvaguarda da integridade dos sistemas, da privacidade da informação, e do cumprimento das leis de *copyright*, licenças e contratos de utilização (para software, música, filmes, artigos…). As regras de conduta na utilização de postos de trabalhos, computadores colocados em espaços públicos e meios de comunicações como a Rede Wireless Eduroam, devem ser cumpridas.

A segurança da informação transmitida através da rede, a sua recolha, armazenamento, categorização e acesso, bem como dos processos de gestão organizacionais e de gestão de segurança da informação são prioridades atuais, tendo em conta que toda a operação diária assenta em recursos tecnológicos. No caso da ESEL, esta vertente assume ainda maior importância, dado que, como instituição de ensino superior, a interação com os estudantes e os processos administrativos, de ensino e aprendizagem tem uma componente *online*, através de sistemas e aplicações baseados no acesso web. O âmbito da segurança não se limita ao espaço físico da ESEL, mas estende-se a todo e qualquer lugar onde trabalhe um estudante ou colaborador.

As pessoas elegíveis a receber uma identidade eletrónica são os estudantes e colaboradores da ESEL. Os detentores de identidade eletrónica da ESEL que utilizem equipamentos pessoais (computadores e outros) são os únicos responsáveis pelos mesmos, não sendo responsabilidade da ESEL a sua manutenção, reparação, atualização ou qualquer outra intervenção técnica.

São aqui definidas as políticas de segurança instituídas na ESEL, que permitem definir responsabilidades, utilizações permitidas e procedimentos de atuação por parte dos vários tipos de utilizadores.

REGRAS DE UTILIZAÇÃO

A Rede da ESEL é partilhada por uma larga comunidade de utilizadores. As regras de utilização têm por objetivo ajudar os utilizadores a fazerem uso dos recursos computacionais e de rede de forma responsável, segura e eficiente, contribuindo desta forma para maximizar a disponibilidade desses mesmos recursos. Seguir as regras de utilização ajudará a maximizar o acesso a esses recursos e a assegurar que todos os utilizadores agem de forma responsável, legal e com respeito pela privacidade dos outros. É importante notar que as Redes de acesso *wireless* fazem igualmente parte das infraestruturas de comunicações da ESEL, e como tal os utilizadores devem obedecer às mesmas regras na utilização destas redes.

É assumido que as regras de utilização são respeitadas e seguidas por todos os utilizadores da Rede.

A violação de qualquer uma das regras expressas neste documento pode sujeitar o utilizador em causa a procedimentos punitivos. As punições poderão variar de acordo com a gravidade da ocorrência verificada, podendo corresponder ao cancelamento da conta do utilizador, ou a procedimentos disciplinares.

Note que as leis sobre privacidade, *copyright*, roubo, ameaças, etc. são igualmente aplicáveis aos utilizadores de computadores. Essas leis aplicam-se a todos os membros da sociedade independentemente do meio de comunicação utilizado: pessoalmente, telefone ou computador. Por sua vez as entidades judiciais estão cada vez mais alerta e ativas perante as violações levadas a cabo por parte de utilizadores de computadores. As regras de utilização definidas pela FCT/FCCN para a Rede Académica RCTS também se aplicam aos utilizadores da Rede da ESEL, visto a conectividade Internet da ESEL ser assegurada por esta Instituição.

INCUMPRIMENTO DA POLÍTICA DE SEGURANÇA

O não cumprimento destas políticas resultará em sanções administrativas, podendo ser vedado o acesso de forma temporária ou definitiva à conta de utilizador em casos que coloquem em causa a segurança da informação institucional. Casos que resultem em acesso indevido a informação, tentativas de utilização de técnicas informáticas ou de engenharia social para acesso aos sistemas da ESEL, motivarão o contacto com as autoridades.

Casos que não respeitem leis de *copyright* (direitos de autor) poderão resultar em processos civis ou criminais.

DEFINIÇÃO DE POLÍTICA DE GESTÃO DE USERNAMES E PASSWORDS

A autenticação nos sistemas de informação é baseada numa palavra-passe (senha ou password).

SEGURANÇA DA PALAVRA-PASSE (PASSWORD)

GESTÃO DA PALAVRA-PASSE

Todos os alunos e colaboradores têm um identificador, pessoal e intransmissível e uma palavra-passe confidencial, que os identificará univocamente.

CARACTERIZAÇÃO DA PALAVRA-PASSE

A palavra-passe escolhida pelo utilizador deverá obedecer aos seguintes critérios de complexidade:

- Deverá conter pelo menos 6 caracteres, e no máximo 12;

- Deverá conter pelo menos um caracter de 3 das 4 seguintes categorias:

  - Um caracter maiúsculo: (A até Z);

  - Um caracter minúsculo: (a até z);

  - Um caracter numérico: (0 até 9);

  - Um caracter especial: (~ ! @ # $ % ^ & * _ - + = ` | ( ) { } { } : ; " ' < > , . ? /)

  - Não poderá fazer referência ao *username* escolhido nem ao nome do utilizador.

Abaixo, encontram-se identificadas algumas boas práticas a ter em consideração, para definição/manutenção da palavras-passe:

- As palavras-passe não devem ser baseadas em expressões facilmente descobertas por terceiros ou obtidas através de informação pessoal (ex. nomes, números de telefone, datas de nascimento, etc.);
- Uma palavra-passe nunca deve ser partilhada com outra pessoa sob nenhum pretexto.

USO DA PALAVRA-PASSE

Cada utilizador é responsável pela sua identidade e credenciais de acesso. A identidade digital proporcionada pelas credenciais da ESEL identifica, perante a ESEL, a pessoa a quem foi atribuída.

Fornecer a sua *password* a alguém é como oferecer-lhe um cheque em branco e assinado por si, ou o seu cartão de crédito. Não deve em caso algum fazê-lo, mesmo que apenas pretenda disponibilizar o uso da sua conta temporariamente. Qualquer pessoa que tenha acesso à sua *password* poderá fazer uso da sua conta, e tudo o que essa pessoa faça que viole as regras de utilização em vigor ficará registado. Com base nesses registos ser-lhe-á imputada responsabilidade a si. Lembre-se, portanto, que se a sua conta for utilizada de forma abusiva a responsabilidade será sua. Note que isto aplica-se igualmente à partilha de *passwords* para acessos a Redes wireless. A sua *password* dá acesso a um conjunto alargado de serviços na Rede da ESEL e qualquer procedimento abusivo (incluindo procedimentos no âmbito da utilização de Redes wireless) ser-lhe-á imputado legalmente.

Todos os utilizadores devem alterar a palavra-passe entre 1 a 2 vezes por ano.

Caso se suspeite de má utilização ou usurpação de identidade, a respetiva conta é imediatamente bloqueada.

PROTEÇÃO DE EQUIPAMENTO EXTERNO À ESEL

Cada utilizador é responsável pelo bom uso dos seus equipamentos e pelas consequências resultantes da má utilização dos mesmos.

Os utilizadores devem garantir que o equipamento não vigiado tem uma proteção adequada, adotando as seguintes medidas:

- Os postos de trabalho requerem um nível mínimo de proteção (ex. Proteção de ecrã mediante palavra-passe);
- Sempre que o utilizador abandone o posto de trabalho, mesmo que por um curto espaço de tempo, deve bloquear as sessões abertas nos sistemas (Win + L);
- As sessões ativas nos sistemas devem ser terminadas, quando o trabalho é concluído.

POLÍTICA DE E-MAIL

- Não abra anexos de e-mail, se não tiver certeza absoluta de que solicitou esse email, ou que provém de fonte fidedigna;
- Desconfie de todas as mensagens de e-mail com assuntos estranhos, ou de remetentes que não conhece;
- Não reenvie e-mails do tipo corrente, aviso de vírus, avisos da Microsoft/AOL/Symantec, criança desaparecida, criança doente, pague menos em alguma coisa, não pague alguma coisa, etc.

POLÍTICA SOCIAL

A segurança da informação não é um problema exclusivamente tecnológico e só é eficaz se se observarem regras de comportamento social, que não invalidem as soluções tecnológicas adotadas, nomeadamente:

- Não partilhe a sua palavra-passe com ninguém. As equipas de suporte informático e tecnológico da ESEL nunca irão pedir a sua palavra-passe, pelo que desconfie de qualquer pedido neste sentido, efetuado por e-mail ou qualquer outro meio;
- Não utilize a sua senha em outros computadores ou sites que não correspondam a serviços da ESEL, ou federados (ex. Eduroam, Colibri são serviços com autenticação federada de uso sancionado pela ESEL);
- Apenas aceite ajuda técnica de um membro das equipas de suporte informático;
- Relate às equipas de suporte informático pedidos externos ou internos, ou situações de que tenha conhecimento, que não estejam de acordo com as normas especificadas neste documento.

VÍRUS E CÓDIGOS MALICIOSOS

- Mantenha o seu antivírus atualizado;
- Ao utilizar CDs, DVDs ou pen-drives de fora da instituição, efetue a verificação dos mesmos pelo programa de antivírus. Se forem detetados vírus ou outras ameaças, abstenha-se de usar os meios infetados;
- Não abra ficheiros recebidos por e-mail de entidades que não conhece, ou com assuntos estranhos;
- Não execute ficheiros descarregados de sites que não correspondem ao esperado. Por exemplo, se está a tentar descarregar um documento PDF e, na realidade, o ficheiro descarregado é um executável (extensão .exe, .bat ou .com), a probabilidade de possuir código malicioso ou intrusivo é muito alta, pelo que deve apagá-lo imediatamente;
- Note que, com a crescente complexidade dos formatos de representação da informação, não são apenas os ficheiros executáveis (.exe, .bat ou .com) que podem albergar códigos maliciosos. Ficheiros de tipo .doc, .pdf, .jpg, entre outros, podem causar problemas desta natureza.

POLÍTICA DE PRIORIDADE DE TRÁFEGO

É dada prioridade ao tráfego de rede para acesso a aplicações e sistemas internos da ESEL, enquadrados com os objetivos da Instituição. Todo o tráfego de acesso a sites ou serviços disponibilizados por terceiros, a partir da Internet, ficará sujeito à largura de banda restante, sendo a velocidade de transmissão e receção de dados a melhor possível após a passagem do tráfego prioritário. Não é garantido assim o acesso rápido a serviços que não sejam considerados críticos aos objetivos da ESEL (por exemplo: serviços de vídeo e rádio em *streaming*). A ESEL reserva-se o direito de bloquear o acesso a sites externos, no âmbito da gestão de tráfego de rede, com o intuito de proporcionar as melhores condições de trabalho e de segurança aos seus utilizadores.

CONTACTOS

Poderá contactar a ESEL para assuntos relacionados com a utilização da Rede através do contacto informatica@esel.pt.