Direção de Sistemas de Informação

REGULAMENTO "POLÍTICA DE UTILIZAÇÃO DE EQUIPAMENTO INFORMÁTICO, *SOFTWARE* E INTERNET"

RG-PR08-01/V04

Regulamento aprovado pela Presidência do Instituto Superior de Economia e Gestão

2013-10-23

Índice

1. Introdução

Estas regras foram emitidas pela Presidência do ISEG em consonância com os seus princípios, tornando-se obrigatórias para todos os seus utilizadores (pessoal docente, não docente, alunos ou terceiros devidamente autorizados) a aceder a qualquer sistema ou tecnologia de informação, pertença ou meramente operado no ISEG.

Esta política aplica-se a todos os utilizadores que têm acesso a qualquer sistema ou tecnologia de informação que pertença ou seja manipulado no ISEG, estendendo-se a sua aplicação a esses equipamentos onde quer que estejam situados.

Todas as referências neste documento para a Direção de Sistemas de Informação do ISEG (DSI/ISEG) serão entendidas como referência à própria DSI/ISEG e seus colaboradores diretos.

O propósito desta política é proteger os ativos de informação detidos e utilizados pelo ISEG de todas as ameaças, internas ou externas, deliberadas ou acidentais e satisfazer todas as exigências regulamentadas e/ou legisladas, especificamente:

- Convenção de Berna - 1971
- Lei da Proteção de Programas de Computador (CE) – 109/1991
- Lei de Proteção Jurídica dos Programas de Computador – 252/1994
- WIPO-World Intellectual Property Organization - Copyright Act (Genebra) - 1996
- Livro Verde relativo à Convergência dos Sectores das Telecomunicações, dos meios de Comunicação Social e das T.I.'s e às suas implicações na regulamentação - rumo à Sociedade de Informação - 1997
- Livro Verde sobre a Patente Comunitária - 1997
- Lei da Proteção Legal das Bases de Dados – 1998
- Lei dos Dados Pessoais e Privacidade nas Comunicações Eletrónicas - 2012

Esta política é parte da iniciativa da DSI/ISEG em cumprir as boas práticas do sector (ITIL, ISO 27001), estabelecendo as regras que devem ser observadas durante o uso da informação da organização. Tem ainda o intuito de resguardar tanto os pilares básicos (Confidencialidade, Integridade, Disponibilidade), como seus derivados (e.g. Autenticidade, Não-Repúdio, Propriedade).

Qualquer suspeita ou efetiva fuga a esta regra interna, que possa afetar sistemas e tecnologias de informação do ISEG, será devidamente investigada pelos Serviços de informática e Jurídicos internos ou por terceiros especialmente contratados para o efeito. Poderá ser aplicada uma ação disciplinar que pode em última instância conduzir a processo disciplinar, não impedindo contudo uma ação criminal.

No caso de qualquer dificuldade na interpretação desta regra interna, a mesma deverá ser resolvida recorrendo à DSI ou diretamente à Presidência do ISEG.

Esta política será publicada nos procedimentos internos do ISEG e na Intranet. Qualquer aditamento ou revisão será comunicado a todo o pessoal através de correio eletrónico ou qualquer outra forma escrita.

2. *Software* protegido pelo direito de autor

2.1. A lei do direito de autor que regulamenta o uso de propriedade intelectual, incluindo o *software*, refere que é ilegal copiar qualquer peça de *software* a menos que expressamente permitido pelo legal detentor dos direitos de autor.

2.2. Todo o *software* tem um contrato de licenciamento associado, o qual vincula a sua utilização. Em caso de dúvidas, deverá o/a utilizador/a consultar a documentação da aplicação em causa ou contactar a DSI, caso as dúvidas persistam após leitura da mesma.

2.3. A Direção de Sistemas de Informação assegurará que são conhecidas todas as condições aplicáveis ao licenciamento do *software* em uso pelos utilizadores.

2.4. Se for provado que foram utilizadas cópias ilegais de *software,* o ISEG não só pode enfrentar um processo-crime seguido de um cível, mas também podem ser envolvidos nestes processos os dirigentes do ISEG e os colaboradores que individualmente, ou em coletivo, tiveram ação no processo, ficando solidários perante a responsabilidade criminal e cível.

2.5. Cópias legitimas de *software* serão entregues prontamente a todos os utilizadores que delas necessitem, sujeitas ao processo de autorização necessário, e logo que o mesmo tenha sido obtido.

2.6. Nenhum/a colaborador/a do ISEG (exceto a DSI) deverá fazer ou executar de qualquer forma cópias de *software*.

2.7. O ISEG não permite o uso de cópias não autorizadas de *software*. Qualquer colaborador que reproduza *software* ilegalmente ficará sujeito às penalidades expressas na lei.

2.8. É interdito a qualquer colaborador/a proporcionar o acesso a qualquer *software* pertença do ISEG a terceiros.

2.9. Todo o *software* deve ser adquirido por recomendação da DSI, que instalará os programas nos computadores designados ou nos servidores.

2.10. Um registo de todo o *software* autorizado será mantido pela DSI. Todas as licenças e suportes informáticos serão guardados centralmente. Os manuais impressos serão enviados para a Biblioteca do ISEG, para disponibilização ao público.

2.11. A DSI ficará responsável pelo registo e atualização de todo o *software* conforme fornecido pelos respetivos fornecedores, instalando as atualizações consoante venham a ser disponibilizadas, mantendo o controlo de todas as versões disponíveis no ISEG.

2.13. Não é permitido ao utilizadores trazer *software* de casa e instalá-lo em qualquer computador do ISEG.

2.14. A instalação de aplicações de terceiros ou jogos não é permitida em qualquer computador do ISEG.

2.16. O uso de *freeware* ou *shareware* registado só deverá ser permitido para propósitos do trabalho do ISEG. Tendo em conta que é autorizado, deve ser providenciado e instalado pela Direção de Sistemas de Informação.

2.17. Todos os computadores do ISEG serão auditados regularmente, como parte das condições de alcançar e manter a credenciação do ISEG perante as entidades que zelam pelos Direitos de Autor.

3. Segurança

3.1. O ISEG tem procedimentos para lidar com a ameaça de vírus, o risco de roubo de *hardware* e *software*, o acesso não autorizado de dados e a manutenção e segurança dos sistemas.

3.2. Os colaboradores não podem revelar qualquer informação relativa às facilidades das Tecnologias de Informação do ISEG perante qualquer pessoa ou entidade exterior, sem a permissão expressa da Presidência do ISEG. Qualquer pedido neste sentido deverá ser passado diretamente para a Direção de Sistemas de Informação.

3.3. A todos os utilizadores de computador são consignados um *username* e uma palavra-chave que são únicas e que não devem ser compartilhadas com qualquer outro colaborador.

3.4. As palavras-chave não devem ser escritas, ou deixadas onde outros as possam encontrar.

3.5. As palavras-chave devem ser difíceis de adivinhar e conter oito caracteres no mínimo, incluindo alguns números e caracteres especiais tais como ! # £ $.

3.6. As palavras-chave devem ser mudadas em intervalos regulares. O *Helpdesk* ajudá-lo(a)-á demonstrando como fazer isto se tiver alguma dificuldade.

3.7. Nunca deixe um computador ligado à rede desacompanhado com a palavra-chave introduzida.

3.8. É considerado crime tentar ter acesso deliberado a um sistema para o qual não tenha autorização.

3.9. A Direção de Sistemas de Informação verifica regularmente todos os sistemas e eventuais tentativas de acesso não autorizado aos mesmos. Qualquer tentativa de acesso não autorizado é investigada.

3.10. Os *laptops* não devem ficar desacompanhados em qualquer local, nunca deixados à vista dentro de viaturas, transportes públicos ou hotéis.

3.11. Só a colaboradores afetos à Direção de Sistemas de Informação é permitido mover qualquer equipamento, dentro ou fora dos edifícios ou para outro local.

3.12. Nenhum dispositivo periférico (máquinas fotográficas digitais, PDA's, etc.) pode ser instalado ou configurado em qualquer computador do ISEG, exceto pela Direção de Sistemas de Informação.

3.13. A obsolescência de equipamentos informáticos é determinada pela DSI, a qual, sempre que se justifique, solicita a remoção/destruição desse equipamento à Divisão de Logística e Apoio Técnico, de acordo com as leis ambientais. Em coordenação com os Serviços Financeiros, procede à atualização dos registos de *hardware* e *software* apropriados.

4. Utilização de Aplicações

4.1. O ISEG dispõe de aplicações desenvolvidas à sua medida, exclusivamente para utilização no âmbito das atividades oficiais do ISEG.

4.2. O acesso às aplicações do ISEG será atribuído tendo em conta as necessidades inerentes ao seu estatuto e área de atividade na Escola. O ISEG reserva o direito de proceder judicialmente contra qualquer indivíduo ou instituição que tente obter um acesso por vias ilícitas.

4.3. Os utilizadores das aplicações do ISEG deverão garantir a integridade dos dados nelas contidos e introduzidos, salvaguardado a sua confidencialidade. Em caso de engano, deverão informar de imediato o seu responsável hierárquico ou a DSI com vista à imediata correção do(s) erro(s).

5. Correio Eletrónico

5.1. O ISEG providencia o uso de um sistema de correio eletrónico para ajudar os seus colaboradores no desempenho do seu trabalho e o seu uso deverá ser limitado às atividades oficiais do ISEG.

5.2. Porém, o uso pessoal e ocasional de correio eletrónico é permitido pelo ISEG, com a compreensão de que as mensagens pessoais serão tratadas como as mensagens empresariais.

5.3. O uso pessoal do sistema de correio eletrónico nunca deverá afetar o fluxo de tráfego normal do correio eletrónico a nível empresarial. O ISEG reserva o direito de remover o correio eletrónico pessoal identificável para preservar a integridade dos sistemas de correio eletrónico.

5.4. Nenhum colaborador, consultor ou fornecedor deve usar o sistema de correio eletrónico de forma a que o mesmo possa ser interpretado como um insulto, ou ofensivo por qualquer outra pessoa, ou Empresa, ou sob qualquer forma que possa ser prejudicial para a imagem do próprio ISEG. Isto tanto no correio eletrónico recebido como emitido.

Exemplos de material proibido incluem: Mensagens sexualmente explícitas, imagens, caricaturas, ou anedotas; Profanação, obscenidade, difamação, ou calúnia; Pronúncias indistintas étnicas, religiosas, ou raciais.

5.5. Todo o correio eletrónico enviado ou recebido será registado e quando considerado apropriado pelo ISEG, pode ser aberto e lido por entidade devidamente autorizada pelo ISEG numa base de confidencialidade absoluta.

5.6. É necessário algum cuidado no envio de mensagens para destinos externos múltiplos. Isto pode ser considerado como *spamming*, uma atividade considerada ilegal em muitos países.

5.7. Para todas as mensagens, deverá lembrar-se que o correio eletrónico não é uma forma segura de comunicação. As mensagens que são enviadas passam por servidores e redes proprietárias de outras pessoas. Se o conteúdo da mensagem pode causar problemas para o ISEG ou perda financeira se os conteúdos se tornarem conhecidos, um método mais seguro deve ser usado.

5.8. Lembre-se de sair da rede quando se ausentar da sua área de trabalho. De modo algum deve enviar correio de um PC onde não fez *login*.

5.9. Os endereços de correio eletrónico não devem ser públicos desnecessariamente. Se coloca o seu endereço durante o preenchimento de pesquisas ou de outros questionários corre o risco de receber correio não desejado.

5.10. Não deverá subscrever listas de correio eletrónico que não sejam aprovadas pelo ISEG. Os volumes de mensagens que podem ser geradas são elevados e o/a utilizador/a, não tendo controlo sobre o seu conteúdo, estará a propiciar o conflito com as condições acima declaradas.

5.11. O correio eletrónico não deve ser usado para enviar grandes arquivos em anexo, a menos que seja muito urgente. Muitos sistemas de correio eletrónico não aceitam grandes arquivos, os quais são devolvidos, podendo resultar em sobrecarga do próprio sistema de correio eletrónico do ISEG. Para enviar grandes quantidades de dados deverão utilizar-se CDs ou DVDs, sempre que possível.

5.12. Não se devem abrir anexos de correio eletrónico (executáveis, essencialmente) a menos que os esteja aguardando, e mesmo assim recomendamos extrema precaução.

5.13. A facilidade de automaticamente enviar correio para contas pessoais não deverá ser usada. O ISEG prevê várias soluções para ter acesso ao correio eletrónico da Escola quando longe do escritório. Se subsistirem dúvidas consulte a Direção de Sistemas de Informação.

6. Internet

6.1. O ISEG providenciará acesso à Internet aos colaboradores no sentido de os ajudar no seu desempenho profissional. Onde este acesso é colocado, subentende-se que o seu uso deverá ser limitado às atividades oficiais do ISEG. Porém é reconhecido que poderá haver ocasiões em que os colaboradores desejam utilizar a Internet por razões pessoais. Esta utilização será permitida, desde que não interfira com o normal funcionamento do Serviço.

6.2. Nenhuma mensagem que possa comprometer ou criar atritos no ISEG, por ser ofensiva ou abusiva, deverá ser colocada na Internet. Material proibido está em igual circunstância.

6.3. A utilização do sistema não deverá ser notada na rede por outros utilizadores. É importante não participar em jogos *online* ou ter canais ativos incluindo qualquer canal de conversação que transmite constantes atualizações frequentes ao seu PC.

6.4. Não deverá visitar locais de *Web* que exibam conteúdos de natureza pornográfica, ou que contenham material que possa ser considerado ofensivo.

6.5. O utilizador deve sair da rede sempre que se ausente do seu local de trabalho. Não deverá navegar na Internet num PC em que não se tenha registado.

6.6. O ISEG faz o controlo de todos os acessos feitos pelos colaboradores e reserva o direito de tornar público o relatório desta informação.