Normativo de Utilização Aceitável de Ativos e Informação

1 Objeto

Este normativo define as regras internas para a utilização correta de ativos e informação (equipamentos informáticos e de comunicações; internet; email) e identifica as medidas a adotar que potenciem a segurança da informação e a proteção de dados pessoais, em conformidade com o estabelecido no Normativo Geral de Segurança da Informação do CENJOR.

2 Âmbito

Este normativo abrange qualquer equipamento capaz de recolher, processar, armazenar, editar, consultar, visualizar ou disponibilizar informação de forma desmaterializada.

3 Destinatários

Este documento é destinado a todos os trabalhadores, colaboradores, formadores, formandos, prestadores de serviços, fornecedores e outras partes interessadas do CENJOR que tenham acesso, direito de uso ou controlo sobre ativos de informação do CENJOR e/ou aos recursos a eles associados.

4 Aplicabilidade do Normativo

4.1 Equipamentos informáticos e de comunicações

O CENJOR dispõe dos seguintes de equipamentos em função da sua tipologia de uso:

Tipologia	Equipamento
Fixo	Computador fixo e respetivo monitor Impressora Fotocopiadora Projetor Telefone de secretária Outros equipamentos afetos à atividade formativa
Móvel	Computador portátil Telemóvel Equipamentos afetos à atividade formativa, nomeadamente: • Máquina Fotográfica • Câmara de filmar • Gravador de Voz • Tripés
Periférico	Disco externo Pen drive Cartão de memória Webcam Teclado Rato Outros equipamentos afetos à atividade formativa

4.2 Categorias os utilizadores e critérios de utilização

Trabalhadores	
Equipamento	**Circunstâncias em que podem ser utilizados/ requisitados**
Computador fixo	Utilização de equipamentos do CENJOR exclusivamente para a atividade profissional do Cenjor
Computador portátil	Utilização de equipamentos do CENJOR exclusivamente para a atividade profissional do Cenjor
Pen drive e Webcam	Pode ou não ser fornecida pelo CENJOR
Impressora	Utilização de equipamentos do CENJOR exclusivamente para a atividade profissional do Cenjor
Telemóvel	Disponibilização à Direção do Cenjor no âmbito profissional
Telefone Fixo de secretária	Utilização de equipamentos do CENJOR exclusivamente para a atividade profissional do Cenjor

Formadores	
Equipamento	**Circunstâncias podem ser utilizados/ requisitados**
Computador fixo	Utilização em contexto formativo e de acordo com o definido no Termo de Compromisso para Prestação de Formação.
Computador portátil	Utilização de equipamento próprio ou mediante requisição, em contexto formativo e de acordo com o definido no Termo de Compromisso para Prestação de Formação.
Pen drive e cartões de memória	Podem ou não ser fornecidos pelo CENJOR no âmbito da formação.
Impressora e fotocopiadora	Utilização no âmbito da atividade formativa.
Equipamentos afetos à atividade formativa, nomeadamente: • Máquina Fotográfica • Câmara de filmar • Gravador de Voz • Tripés • Outros…	Mediante requisição

Formandos	
Equipamento	**Circunstâncias podem ser utilizados/ requisitados**
Computador fixo	Utilização em contexto formativo e de acordo com regras de funcionamento das salas de formação e Normas de Acolhimento dos Formandos
Computador portátil	Utilização de equipamento próprio ou mediante requisição, em contexto formativo e de acordo com as regras de funcionamento das salas de formação e Normas de Acolhimento dos Formandos
Impressora	Utilização exclusiva em contexto formativo
Equipamentos afetos à atividade formativa, nomeadamente: • Máquina Fotográfica • Câmara de filmar • Gravador de Voz • Tripés • Outros…	Mediante requisição

4.3 Utilização dos equipamentos informáticos e de comunicações

Para a garantir a segurança da informação e de modo a salvaguardar o respeito pelo cumprimento das políticas e normas de tratamento de dados, foram estabelecidos os critérios para utilização dos diversos equipamentos e as práticas a obedecer por todos os utilizadores:

4.3.1 Equipamentos fixos

1. Computador fixo
    a. Todos os computadores fixos devem ter de um primeiro nível de segurança, através da utilização de uma palavra-passe necessária para iniciar a sessão e definida de acordo com o estabelecido para a criação de palavra-passe do CENJOR;
    b. Cada trabalhador, colaborador, formador ou formando não pode partilhar a sua conta de utilizador com outros;
    c. Utilizar as plataformas e equipamentos do CENJOR apenas para o envio de e-mails relativos à atividade profissional;
    d. A autenticação utilizada nas diversas plataformas, nunca poderá ser feita de forma automática;
    e. Não é permitido instalar ou desinstalar *software* nos computadores;
    f. Não é permitido desligar ou ligar qualquer cabo conectado ao sistema;
    g. Não é possível alterar a configuração do Sistema Operativo ou de qualquer *software* instalado nos computadores;
    h. Não podem ser utilizadas Pen drives, discos externos ou outros dispositivos de armazenamento pessoal para gravar informação do CENJOR;
    i. Cada formando só pode gravar informação (ficheiros) na pasta de trabalho de cada curso ou numa Pen drive;

j. Qualquer documento gravado fora da respetiva pasta, será automaticamente eliminado quando o formando encerrar o computador;
k. No final das sessões de formação os formados e formadores devem garantir que todo o equipamento fica desligado e em condições de utilização posterior;
l. Qualquer anomalia detetada deverá ser, automaticamente, comunicada ao Serviço de Apoio à Formação.

2. Impressora e fotocopiadora
   a. Deve ser atribuído um código por trabalhador para impressão;
   b. A impressão de documentação confidencial, deve ser acompanhada presencialmente até à conclusão do processo;
   c. Não é permitido que equipamentos que não sejam do CENJOR sejam ligados à rede para impressão;
   d. Devem ser implementadas as opções de configuração de segurança da informação disponibilizadas pelo dispositivo.

4.3.2 Equipamentos móveis

1. Computador portátil
   a. Todos os computadores portáteis devem ter de um primeiro nível de segurança que consiste na utilização de uma palavra-passe para iniciar a sessão, definida de acordo com o estabelecido para a criação de palavra-passe do CENJOR;
   b. Cada trabalhador, colaborador, formador ou formando não pode partilhar a sua conta de utilizador com outros;
   c. É desaconselhada a ligação às redes *wireless* públicas;
   d. A autenticação utilizada nas diversas plataformas, nunca deverá ser gravada nem feita de forma automática;
   e. Utilizar as plataformas e equipamentos do CENJOR apenas para o envio de e-mails relativos à atividade profissional;
   f. Todas as informações descarregadas dos e-mails e/ou plataformas internas, devem ser gravadas diretamente nas pastas respetivas do servidor.
2. Telefone fixo de uso empresarial
   a. Todos os telefones fixos devem conter mecanismos de segurança de acesso ativos (código pin, palavra-passe, reconhecimento facial ou digital, entre outros);
   b. A lista de contactos deve cingir-se exclusivamente aos necessários para o desempenho das funções de cada trabalhador no CENJOR;
   c. Não devem ser instaladas aplicações que não sejam necessárias ao desempenho das funções de cada trabalhador;
3. Equipamentos afetos à atividade formativa
   a. Só é permitida a utilização destes equipamentos, com a devida autorização e o preenchimento do termo de responsabilidade;
   b. Os conteúdos de voz, de imagem ou de vídeo devem ser armazenados no servidor CENJOR, na pasta correspondente, com acesso restrito e o conteúdo duplicado deverá ser eliminado do equipamento;

c. Os equipamentos só podem ser utilizados, quando justificável, para fotografar e/ou para gravar som e/ou vídeo após obtenção do consentimento pelo titular dos dados.

4.3.3 Equipamentos periféricos

1. Disco externo, Pen drive e cartões de memória

a. Não é permitido o uso de periféricos, como Pen drives e discos externos, cuja utilização tenha como objetivo o processamento de informação;

b. Discos externos ou Pen drives que contenham dados pessoais devem estar protegidos por palavra-passe.

4.4 Boas práticas na utilização e segurança dos equipamentos móveis

- Cumprir o estipulado para a criação das palavras-passe;
- Manter o *software* atualizado e instalar todos os mecanismos de segurança disponíveis;
- Fazer, periodicamente, cópias de segurança dos dados;
- Bloquear os equipamentos quando não estão em utilização;
- Acessos remoto: os equipamentos que são utilizados para acesso remoto ao computador/servidor do CENJOR devem estar protegidos contra acesso indevido e a sua utilização tem que ser autorizada pelo Responsável de Segurança de Informação.

4.5 Regras Palavras-passe

A cada utilizador é atribuído um perfil, que define os privilégios atribuídos e uma palavra-passe, pessoal e intransmissível.

Todos os equipamentos informáticos e de telecomunicações devem ter palavra-passe associada para permitir a respetiva utilização.

A criação da palavra-passe deve obedecer às seguintes regras:

Equipamento	Regras
Computadores fixos, portáteis, Pen drives e discos externos	Pode ser constituída por frases ou excertos de texto longo conhecidos pelo utilizador, sem caracter de «espaço». Alfanumérica (mínimo 9 caracteres), com pelo menos 3 dos seguintes conjuntos de caracteres: letras minúsculas e maiúsculas, algarismos e caracteres especiais. As palavras-passe de Administrador de sistemas devem seguir a mesma estrutura, mas com um comprimento de 13 caracteres. Em contexto formativo, formadores e formandos receberão uma palavra-passe de 6 dígitos.
Impressoras, fotocopiadoras	Mediante configuração do próprio equipamento

4.5.1 Segurança na utilização da palavra-passe:

- As palavras-passe são pessoais, intransmissíveis e não podem ser divulgadas;
- O prazo para alteração das palavras-passe deve ser, no máximo, de 6 meses;
- Guardar as palavras-passe em *software*s com encriptação (ex. *KeePass Safe*);
- Memorizar as palavras-passe;
- Não guardar as palavras-passe escritas em papéis ou em locais visíveis;
- Utilizar palavras-passe diferentes para uso profissional e para uso pessoal;
- Não gravar a palavra-passe de forma automática nos sistemas e dispositivos.

4.6 Regras no acesso à Internet e utilização do e-mail

- O acesso à Internet deve ser utilizado de forma a não violar a lei vigente, especialmente a relacionada com o download de conteúdos (e.g. imagens, músicas, vídeos) e software, que deve obedecer às leis de proteção de propriedade intelectual, direitos de autor, copyright e outras aplicáveis;
- O e-mail da organização não poderá ser utilizado para a criação e distribuição de qualquer mensagem perturbadora ou ofensiva, incluindo comentários ofensivos sobre raça, género, traços físicos, deficiências, idade, orientação sexual, pornografia, convicções e práticas religiosas, orientações políticas ou naturalidades;
- O envio de e-mails em volume, i.e., para uma lista de distribuição de grande dimensão, apenas deverá ser efetuado por colaboradores da organização com necessidade desse tipo de comunicação alargada (administração, recursos humanos, comunicação corporativa, etc.);
- O conteúdo das mensagens abrangidas por esta política está igualmente protegido pelas políticas de proteção de informação da organização, na promoção da sua integridade, confidencialidade e disponibilidade. Os utilizadores deverão ter sempre este aspeto em atenção; em particular, em situações de envio de informação para o exterior;
- No reforço do ponto anterior, nunca deverá ser feito o reencaminhamento automático de informação para o exterior. Em particular, o conteúdo de correio eletrónico institucional deverá ser mantido nos servidores oficiais ou em sistemas pessoais onde seja visualizado, mas nunca transferido para outros sistemas externos;
- Se por algum motivo for utilizado um endereço de correio eletrónico da organização para publicar informação num grupo, fórum ou outro serviço público de terceiros, a mensagem deverá incluir um aviso explicitando que as opiniões expressas são pessoais e não necessariamente as da organização, exceto se a publicação for feita no âmbito de atividade profissional;
- Informação classificada como confidencial nunca deverá ser reencaminhada, a não ser que tal seja necessário e crítico para o negócio da organização e a mensagem e respetivos anexos estejam cifrados, não devendo o código de acesso à informação ser comunicado ao destinatário na mesma mensagem que envia a informação e devendo preferencialmente tal código ser enviado através de outra plataforma/meio de comunicação;

- É estritamente proibido que qualquer colaborador envie e-mails, com meios da organização ou de dentro da organização, sem ser através dos sistemas de e-mail autorizados;
- A criação de e-mails fazendo-se passar por terceiro é uma violação grave desta política de segurança e poderá dar origem a procedimentos disciplinares e legais;
- Os colaboradores nunca deverão abrir documentos, ficheiros ou URL's (links) que recebam em anexos de um e-mail cuja origem seja desconhecida ou suspeita, ou de que haja suspeita de que o conteúdo possa ser prejudicial ao bom funcionamento do sistema informático. Estes e-mails deverão ser imediatamente apagados e posteriormente deverá ser esvaziada a pasta "Itens Eliminados". Todos os e-mails de spam, chain letters, e semelhantes deverão ser imediatamente apagados (inclusive da pasta de itens eliminados) e nunca deverão ser reenviados. O Colaborador deverá igualmente reportar de imediato Dep. de Informática qualquer suspeita de que um e-mail recebido possa causar uma quebra de segurança nos sistemas da organização, bem como qualquer suspeita de roubo de password ou de usurpação de identidade;
- Os utilizadores deverão ter precaução antes da abertura de anexos de correio-electrónico recebidos de remetentes desconhecidos ou que de outra forma não são esperados e possam ser suspeitos.

4.7 Uso e divulgação de informação

- Os utilizadores dos ativos e informação do CENJOR podem aceder, usar ou divulgar informação de propriedade do CENJOR, mas somente na medida em que forem autorizados e que tal for necessário para cumprir deveres de trabalho; e as funções profissionais que estão atribuídas.
- Os utilizadores são obrigados a relatar imediatamente o roubo, a perda ou a divulgação de informação confidencial não autorizada pela organização, assim como qualquer outro incidente de segurança da informação e/ou violação de dados pessoais.

5 Entrada em vigor e alterações

O presente normativo de Utilização Aceitável de Ativos e Informação entra em vigor na data da sua aprovação e será revisto sempre que seja considerado necessário e comunicado aos seus trabalhadores/colaboradores/formadores e formandos.

Data de aprovação: 12/07/2023