

Introdução

A IDEPA – Indústria de Passamanarias, Lda, está comprometida com a segurança dos dados, contribuindo para a criação de uma verdadeira cultura educativa no que diz respeito à utilização e proteção da informação digital da Empresa.

1. Objetivo

A presente Política tem como objetivo assegurar que a informação da organização é gerida de forma segura, confidencial, íntegra e responsável, protegendo os dados internos, de clientes, fornecedores e outras partes interessadas.

Esta Política visa:

- Garantir a proteção contra acessos não autorizados, perda ou uso indevido da informação;
- Assegurar o cumprimento de requisitos legais e regulamentares;
- Reforçar o compromisso com práticas éticas e responsáveis.

2. Âmbito

Aplica-se a:

- Todos os colaboradores da organização;
- Fornecedores, prestadores de serviços e parceiros;
- Toda a informação em formato físico ou digital;

3. Princípios

A organização compromete-se com os seguintes princípios:

- Confidencialidade: proteger a informação contra divulgação não autorizada;
- Integridade: garantir a exatidão e fiabilidade dos dados;
- Disponibilidade: assegurar que a informação está acessível quando necessário;
- Responsabilidade: garantir o uso ético e conforme da informação;
- Transparência: assegurar comunicação clara sobre o uso de dados.

4. Compromissos da Organização

4.1 Proteção de Dados

A IDEPA assegura a implementação de medidas técnicas e organizacionais para proteger dados de acessos indevidos definindo as seguintes responsabilidades:

Compromisso dos utilizadores:

- Os utilizadores são responsáveis, por cumprir, e fazer cumprir, as regras, normas e procedimentos estabelecidos no Regulamento Interno;
- Todas as palavras-passe de acesso fornecidas aos utilizadores são pessoais, intransmissíveis e de uso exclusivo dos mesmos, que assumem integral responsabilidade pela sua guarda e sigilo;
- Qualquer vulnerabilidade ou utilização ilícita do sistema informático, quer seja pelo aproveitamento de falhas de segurança, quer pela simples tentativa e erro de acerto de palavra-passe, o poderá estar sujeita às devidas sanções civis e criminais, nomeadamente ao disposto das Leis n.ºs 109/2009, de 15 de Setembro, e n.º 46/2012, de 29 de Agosto, bem como noutras que sejam aplicáveis aos factos que venham a ser apurados.

Responsabilidade de gestão do processo de segurança da informação:

- O Departamento de Sistemas de Informação (DSI) supervisionará o cumprimento das regras do Regulamento. Também será responsável pela implementação das normas de segurança e adoção de medidas técnicas contra todas as infrações cometidas (voluntária ou involuntariamente).
- O DSI será também responsável pela divulgação do regulamento e esclarecimento de dúvidas aos utilizadores;
- O DSI deve assegurar a proteção de dados de clientes e terceiros.

A IDEPA define ainda outros critérios de proteção de dados relacionados com:

Uso da rede interna, hardware e software:

- O uso da infraestrutura tecnológica é disponibilizado exclusivamente como ferramenta de trabalho;
- Toda a rede interna, hardware e software estão sujeitos à monitorização pelo DSI.

Uso e controlo de informações, dados e arquivos:

Sem prejuízo do disposto nos artigos 3.º, 4.º, 5.º e 6.º da Lei 109/2009, de 15 de setembro é estabelecido que:

- Todos os documentos eletrónicos, dados e informações resultantes das atividades exercidas pelos utilizadores e serviços, devem estar armazenados nas pastas de rede K: ou H;;

MP 2 010 Revisão 0 Data: 19/02/2026	POLÍTICA DE SEGURANÇA DE DADOS E GESTÃO RESPONSÁVEL DA INFORMAÇÃO	 THE ACCESSORY IS ESSENTIAL
---	--	---

- Não é permitida a utilização dos postos de trabalho para armazenar dados e documentos pessoais dos utilizadores;
- Os dados constantes nas Bases de Dados utilizadas pelos diversos sistemas aplicacionais da IDEPA, devem ser mantidos íntegros e invioláveis;
- Deve ser garantido o tratamento de dados com base em consentimento quando aplicável.

Direitos de acesso à Internet:

- O acesso a Internet está sujeito a monitorização e filtragem. Existe um servidor responsável por analisar se os conteúdos poderão ou não ser acedidos.

Receção, inserção e envio de arquivos:

- Apenas será permitida a receção de ficheiros para fins de carácter profissional, necessários ao exercício das atividades dos serviços e/ou utilizadores;
- É estritamente proibido o carregamento de qualquer arquivo executável pelos utilizadores, com terminações tais como: .EXE, .COM, .SCR, .ISO ou outras que possam comprometer o sistema através da execução de comandos maliciosos;
- Fica vedada a inserção ou disseminação voluntária e intencional, de ficheiros que contenham vírus ou qualquer espécie de programa nocivo, sob pena de responsabilização civil e criminal, de acordo com a legislação em vigor;
- É proibido o envio de qualquer ficheiro que desrespeite as normas de direitos autorais, que configure prática de infração penal ou ilícito civil e/ou que desrespeite quaisquer outras normas vigentes no momento do envio do ficheiro;
- É proibido o envio de qualquer informação confidencial, salvo devida autorização superior;
- É proibido o envio de quaisquer arquivos que violem direitos de terceiros, ou que possam causar prejuízos, a terceiros e/ou à IDEPA;
- É proibida a cópia de dados ou ficheiros para quaisquer memórias externas;
- É proibido o envio de qualquer arquivo de carácter ilegal, ofensivo e/ou imoral, de forma genérica.

4.2 Gestão de Riscos

Para gestão de riscos associados à segurança da informação, a IDEPA:

- Define critérios relativos à utilização de software e hardware;
- Define procedimentos para uso de equipamentos portáteis e equipamentos de impressão digital;

MP 2 010 Revisão 0 Data: 19/02/2026	POLÍTICA DE SEGURANÇA DE DADOS E GESTÃO RESPONSÁVEL DA INFORMAÇÃO	 THE ACCESSORY IS ESSENTIAL
---	--	---

- Define procedimentos para uso da Internet, estando bloqueada com 96% de confiança a navegação a sites de qualquer tipo de pornografia, partilha de ficheiros, terrorismo, drogas, jogos, violência e agressividade, hackers ou pirataria, música on-line e outros que se considerem desadequados às funções;
- Realiza avaliações periódicas de risco em segurança da informação, quer pela necessidade de utilização de suportes externos, quer pela necessidade de acessos a informação restrita, quer por testes aleatórios realizados ao sistema;
- Cria e monitoriza as contas de e-mail corporativa, através de filtragem de conteúdos. A monitorização será realizada, a qualquer momento e de forma automática. Neste sentido, as mensagens enviadas para um e-mail, poderão ser redirecionadas para outro e-mail interno, na sequência de suspeita de conter conteúdo malicioso, sem necessidade de qualquer aviso prévio e sem conhecimento do emissor e do recetor da mensagem;
- Define critérios para utilização de contas de e-mail particular, devendo, nos casos em que há autorização específica, obedecer aos padrões de segurança definidos pela IDEPA;
- Identifica e mitiga vulnerabilidades.

4.3 Gestão de Incidentes

A Idepa compromete-se a:

- Implementar um plano de resposta a incidentes com base num sistema de backups:
 - Cópia diária para unidade de discos do servidor local e unidade externa dedicada à gestão de backups (StoreOnce);
 - Cópia incremental / total para tape;
 - Réplica online dos servidores principais;
 - Procedimento diário de controlo de back-ups.
- Garantir a comunicação e tratamento adequado de incidentes.

4.4 Controlo de Acessos

O controlo de acessos define, ao nível do utilizador ou grupos de utilizadores, as permissões e restrições no acesso aos documentos e informação existente nos servidores.

As permissões ou restrições no acesso à informação são definidas pela Gerência, que informa o responsável do departamento de Sistemas de Informação sobre o tipo de acesso a ser configurado ou alterado para determinado utilizador ou grupo de utilizadores.

Pretende-se com o controlo de acessos:

- Limitar o acesso à informação com base na “necessidade de saber”;
- Definir perfis de acesso e autenticação segura nas aplicações utilizadas para o desempenho da atividade profissional dos colaboradores;

- Controlo dos contratos de licenciamento ou licenças avulsas, impedindo a instalação de qualquer tipo de aplicação informática e gerindo a instalação de todos os programas licenciados.

4.5 Gestão de Informação e Registos

A IDEPA compromete-se a:

- Garantir controlo documental e gestão de registos conforme, de acordo com que se encontra definido no Manual da Qualidade;
- Definir critérios de retenção e eliminação segura de dados.

4.6 Formação e Sensibilização

Sempre que existe admissão de novos colaboradores é promovida a formação em segurança da informação, através da sensibilização para as boas práticas e riscos associados, sendo feita uma abordagem à esta política e distribuído o regulamento interno de segurança de sistemas de informação.

4.7 Gestão de Terceiros

A IDEPA compromete-se a:

- Avaliar fornecedores quanto à segurança da informação;
- Garantir cláusulas de confidencialidade e proteção de dados.

4.8 Canal de Denúncias

A IDEPA disponibiliza mecanismos seguros, acessíveis, confidenciais e, sempre que legalmente permitido, anónimos para a comunicação de preocupações, reclamações ou denúncias relacionadas com irregularidades ou incumprimento da segurança de dados, garantindo a proteção do denunciante.

As comunicações podem ser efetuadas através dos seguintes canais:

Canal de Denúncias:

<https://canaldenuncias.idepa.com/>

Carta endereçada aos responsáveis de Departamento Administrativo-Financeiro e RH:

- Recursos Humanos: Andreia Oliveira
- Departamento Administrativo/ Financeiro: Victor Lourenço

4.9 Auditoria e Melhoria Contínua

A IDEPA assegura a realização de auditorias periódicas aos sistemas e procedimentos e promove a melhoria contínua do sistema de gestão de informação.

5. Responsabilidades

Cabe à gerência assegurar os recursos necessários e compromisso estratégico e ao responsável pelo DSI a implementação dos meios de controlo e monitorização bem como o cumprimento normativo.

O departamento de RH será responsável pela gestão de eventuais denuncia relativas à segurança de dados ou incumprimento normativo.

Os colaboradores são responsáveis por cumprir as regras de utilização da informação definidas no Regulamento interno e alinhadas com esta política.

6. Cumprimento

O incumprimento desta Política poderá resultar em medidas disciplinares, nos termos definidos no Código de Ética da organização.

Os casos de incumprimento desta política ficam sujeitos às penalidades previstas na Legislação em vigor, nomeadamente as Leis de Proteção de Direitos de Autor, Lei de Software, Lei da Criminalidade Informática, ou outras que se apliquem aos factos que se venham a apurar.

7. Revisão

A presente Política será comunicada e disponibilizada a todos os colaboradores, bem como às restantes partes interessadas relevantes, através dos meios internos e externos considerados adequados, assegurando a sua compreensão e aplicação em toda a organização. A Política será revista, no mínimo, anualmente ou sempre que ocorram alterações significativas na legislação aplicável, nos requisitos das partes interessadas, nos riscos identificados ou na estratégia da organização.

Esta Política foi formalmente aprovada pela Direção da IDEPA.

Aprovado por:

Direção da IDEPA

Nome: _____

Cargo: _____

Assinatura: _____

Data de aprovação: ____ / ____ / ____