ediprinter

SOFTWARE DEVELOPMENT
SINCE 1990

Política de Segurança da Informação

(Versão Resumida)

EDI_SI_PSI_R_PT

Versão: 1.0

Data da última revisão: 12/05/2026

Estado: Aprovado

Responsável/Owner: RSGSI

Índice

1. Objetivo

A Política de Segurança da Informação serve de base ao sistema de gestão de segurança da informação, respeitando a norma internacional ISO/IEC 27001:2022, as normas comunitárias e a legislação e recomendações nacionais específicas em matéria de segurança da informação.

A EDIPRINTER, ao estabelecer o SGSI, assume a presente política, os compromissos nela definidos, a integração dos requisitos do SGSI nos processos da organização e assegura que os recursos necessários à sua implementação estão disponíveis.

2. Audiência

A Política de Segurança da Informação da EDIPRINTER destina-se a todas as partes interessadas, nomeadamente colaboradores, fornecedores, clientes e parceiros. Todas as partes interessadas devem conhecer e agir em conformidade com a Política de Segurança da Informação da EDIPRINTER e com os documentos relacionados, conforme aplicável e adequado. As partes interessadas abrangidas pelo SGSI e que deliberadamente violem esta ou outras políticas associadas ficam sujeitas às consequências aplicáveis, podendo estas ir até à cessação do contrato e/ ou à participação às autoridades policiais ou judiciais das situações que indiciem a prática de crime.

3. Valor da Informação

A informação pode adotar diversas formas (impressa ou escrita em papel, armazenada eletronicamente, transmitida por correio ou meios eletrónicos, entre outras), devendo ser adequadamente protegida independentemente do seu meio, utilização ou suporte. A segurança da informação deverá ser ajustada face à sua importância e valor. O responsável da segurança de informação ou os responsáveis das unidades de negócio com responsabilidade para tal poderão permitir o acesso à informação às partes interessadas de acordo com os procedimentos definidos.

O acesso à informação é um aspeto importante do funcionamento da EDIPRINTER, dependendo da disponibilidade das infraestruturas e dos sistemas de informação a eficiência do serviço prestado aos seus clientes. A segurança no tratamento e transmissão da informação é assim um fator vital para manter a sua eficiência.

Qualquer interrupção do serviço, fuga de informação para entidades não autorizadas ou modificação não autorizada de dados, pode levar a uma perda de confiança e/ou violar as obrigações para com as partes interessadas.

A segurança da informação é um pressuposto fundamental para o sucesso dos serviços prestados pela EDIPRINTER sendo da responsabilidade de todos os colaboradores, fornecedores ou outras entidades, contribuírem proactivamente para a proteção ou partilha de informação sensível por qualquer meio, inclusive verbalmente.

4. Importância da Segurança da Informação

A informação gerida pela EDIPRINTER, bem como os seus processos de suporte, sistemas, aplicações e redes são ativos valiosos que devem ser adequadamente protegidos. A perda de confidencialidade, integridade e disponibilidade podem levar à perda de credibilidade dos serviços prestados pela EDIPRINTER.

Deve ser assegurada a manutenção, de forma permanente e equilibrada, de um nível de qualidade e segurança elevado, prevenindo a materialização de riscos inerentes, para mitigar os potenciais danos provocados pela exploração de vulnerabilidades e incidentes de segurança, e garantir que o negócio opera conforme esperado ao longo do tempo.

As ameaças à segurança da informação estão em constante evolução, o que implica a adaptação contínua de medidas de segurança de modo a acompanhar as alterações tecnológicas, legislativas e/ou sociais. As medidas de segurança devem ser técnicas, economicamente viáveis e não devem limitar de forma inadequada a produtividade e eficiência da EDIPRINTER.

Neste sentido, esta Política estabelece as linhas orientadoras para a efetiva gestão da segurança de informação nas seguintes vertentes:

- Gestão de pessoas: a Segurança de Informação é aplicável a todos os colaboradores da EDIPRINTER e deve ser aplicada de forma transversal em todos os Departamentos e unidades de negócio, devendo ser determinadas as responsabilidades específicas a determinadas funções;
- Gestão do risco: Todos os sistemas (existentes ou planeados) devem ter um nível de segurança adequado face ao risco que a EDIPRINTER está disposta a assumir. Uma análise de risco deve traduzir as preocupações de índole técnica de modo que estas sejam facilmente interpretadas pelo negócio;
- Definição de responsabilidades: A responsabilidade pela qualidade, acessos, utilização e salvaguarda da informação contida nos sistemas é dos Responsáveis desses dados.

Cabe à EDIPRINTER definir as normas e procedimentos que implementem os níveis de segurança da informação definidos pelas entidades proprietárias da informação e vigiar a sua efetividade.

- Regras de segurança: Devem existir políticas de segurança que definam os objetivos a atingir por todos os sistemas de informação, independentemente do seu ambiente;
- Procedimentos de segurança: Desenvolvimento de procedimentos detalhados que definam "o quê" e "como" atingir o nível de segurança pretendido;
- Operação adequada futura dos sistemas de informação: As operações dos sistemas de informação devem estar devidamente documentadas, assegurando que a qualquer momento é possível aferir "quem" e "quando" faz "o quê";
- Fazer o que está correto: A segurança da informação é uma responsabilidade da EDIPRINTER.
- Saber o que está a acontecer: A implementação de controlos que enderecem os riscos aos quais o negócio se encontra exposto, só é eficaz se existir uma adequada monitorização dos controlos, de forma a avaliar, se os mesmos se encontram ajustados face aos objetivos definidos. Igualmente, devem estar definidas ações de resposta atempada quando se verifique a não operacionalidade dos controlos.

5. Modelo de Segurança da Informação

O modelo da segurança de informação da EDIPRINTER tem como compromisso:

- Confidencialidade: garantia de que a informação está acessível apenas por pessoas devidamente autorizadas para o efeito;
- Integridade: salvaguarda da exatidão da informação e dos métodos de processamento;
- Disponibilidade: garantia de que utilizadores autorizados têm acesso à informação sempre que necessário.

Todos os mecanismos de segurança existentes na EDIPRINTER endereçam a confidencialidade, integridade e disponibilidade da informação, devem ser regulados por um corpo normativo constituído por políticas, normas e procedimentos de segurança, encontrando-se estruturado de acordo com o Manual do Sistema de Gestão de Segurança de Informação.

6. Objetivos de Segurança da Informação

- Reforçar o conhecimento e as práticas dos colaboradores sobre segurança da informação;

- Implementar com sucesso a norma ISO 27001;

- Identificar, avaliar e mitigar riscos de segurança para garantir um nível de risco aceitável;

- Detetar, responder e recuperar de incidentes de segurança de forma atempada.

7. Responsabilidade na Segurança da Informação

A Política de Segurança da Informação deve ser implementada por todos os Departamentos e unidades de negócio da EDIPRINTER referidos anteriormente, em conjunto com o IT. As Políticas para a Segurança de Informação definem os objetivos de controlo tal como devem ser aplicados a todos os departamentos da EDIPRINTER.

A gestão de topo compromete-se a satisfazer os requisitos de segurança de informação aplicáveis e a melhorar continuamente o Sistema de Gestão da Segurança de Informação. A estrutura de gestão e coordenação da implementação do Sistema de Gestão de Segurança da Informação é liderada pelo Responsável pela Segurança da Informação e seu backup.

8. Manutenção e Comunicação das Políticas de Segurança

As políticas e normas de segurança de informação devem ser revistas anualmente garantindo que continuam a ser relevantes e adequadas para a EDIPRINTER, devendo ainda ser do conhecimento de todos os colaboradores dentro de cada âmbito de aplicação. Neste sentido, deverão ser definidos quais os procedimentos necessários para a sua revisão e divulgação:

- Assegurar que as políticas são observadas e revistas, caso necessário, para se manterem adequadas à realidade da EDIPRINTER;
- Assegurar a disponibilização de toda a documentação aos colaboradores dentro do seu âmbito de aplicação.
- Assegurar a comunicação eficaz das políticas e normas de segurança de informação a todos os colaboradores de modo que, estes fiquem cientes das suas obrigações individuais no âmbito da segurança da informação.

9. Melhoria Contínua do Sistema de Segurança da Informação

O controlo de segurança da informação das operações de inserção / recolha, processamento, armazenamento, transferência, relacionamento, pesquisa e destruição da informação é tão ou

mais importante do que a funcionalidade de um sistema de informação. Deve, assim, ser assegurada a manutenção permanente e equilibrada de um nível de qualidade e segurança elevados, prevenindo a materialização de riscos inerentes para mitigar/ limitar os potenciais danos provocados pela exploração de vulnerabilidades e incidentes de segurança da informação.

10. Programa de Auditorias e Âmbito

Existe um plano de auditorias definido (documento: "Programa de Auditorias Anual"), onde se encontram programadas as auditorias realizadas ao SGSI. Estas auditorias têm como objetivo garantir a conformidade e melhoria contínua do sistema.

11. Critérios para Equipa Auditora

Estão definidos os critérios da Equipa Auditora (EA) e é selecionada pelo responsável de segurança de informação em conjunto com a Administração, de forma a assegurar o cumprimento do programa e tendo em conta os seguintes requisitos definidos.