Política de Segurança da Informação

Sistema de Gestão de Segurança da Informação

Controlo de Versões

Versão	Data	Descrição Alterações	Criado Por	Aprovado Por
1.0	Julho 2026	Criação do documento	Marco Monteiro António Rocha	Gestão

Índice

1 Âmbito e Objetivo

O presente documento define o Sistema de Gestão de Segurança da Informação (SGSI) da Ambidata Lda. e da Ambidata Espana, doravante designadas como Ambidata Group, estabelecido em conformidade com os requisitos da NP EN ISO/IEC 27001.

1.1 Âmbito do SGSI

O âmbito do SGSI da Ambidata Group abrange a totalidade da organização, incluindo todos os processos, colaboradores, sistemas de informação, infraestrutura tecnológica e ativos de informação associados à seguinte atividade:

"Desenvolvimento e inovação na criação, fornecimento, consultoria e assistência técnica de soluções de Software."

Este âmbito engloba, designadamente:

- Desenvolvimento e manutenção de soluções de software;
- Prestação de consultoria técnica a clientes;
- Suporte e assistência técnica pós-implementação;
- Todos os processos de suporte organizacional que tratam informação sensível da empresa, dos seus colaboradores e dos seus clientes.

O SGSI aplica-se a todas as instalações físicas, sistemas e plataformas tecnológicas utilizados pela Ambidata Group no âmbito da sua atividade, independentemente da sua localização.

1.2 Objetivo do SGSI

O SGSI tem como objetivo assegurar a proteção da informação da organização e das partes interessadas, garantindo a sua confidencialidade, integridade e disponibilidade, através de uma abordagem sistemática de identificação, avaliação e tratamento dos riscos de segurança da informação.

Este sistema visa ainda:

- Promover a melhoria contínua das práticas de segurança da informação;
- Reforçar a confiança dos clientes, parceiros e demais partes interessadas;
- Assegurar a conformidade com os requisitos legais, regulamentares e contratuais aplicáveis;
- Garantir a capacidade de prevenção de incidentes, a disponibilidade e a continuidade da atividade da Ambidata Group.

2 Segurança da Informação

A utilização eficiente da informação deve ser parte indissociável da doutrina e prática quotidiana de uma organização, sendo considerada como componente vital ao êxito do seu trabalho. As políticas de segurança da informação abrangem bases de dados, ambientes informáticos, documentos, arquivos e restantes ferramentas tecnológicas e aplicacionais que envolvam a estrutura de negócio da Ambidata Group.

A Segurança da Informação define-se como a preservação dos seguintes princípios fundamentais:

Confidencialidade	Assegurar que a informação apenas é disponibilizada a quem tem a devida autorização.
Integridade	Assegurar a consistência e veracidade da informação e respetivos métodos de processamento.
Disponibilidade	Assegurar que a informação está disponível a utilizadores com a devida autorização, sempre que este acesso for necessário.
Auditabilidade	Os dados e informações corporativas devem ser registados, compilados, analisados e revelados de modo a permitir que auditores internos ou externos possam atestar a sua veracidade.
Rastreabilidade	Assegurar a capacidade de recuperação do histórico das ações concretizadas, através de um registo atualizado e disponível em qualquer momento.

A informação é um ativo tão importante como qualquer outro ativo da organização, pelo que tem de ser protegida da forma mais apropriada. A Segurança da Informação protege a informação contra uma multiplicidade de ameaças, assegurando a continuidade do serviço, minimizando os efeitos negativos no negócio e melhorando a qualidade do serviço prestado.

3 Necessidade da Implementação de Políticas de Segurança

A informação e os seus processos de apoio, sistemas e redes, são bens essenciais ao negócio de uma organização que desenvolve, implementa e faz a manutenção de software. A confidencialidade, integridade e disponibilidade da informação são elementos essenciais para preservar a competitividade, a rentabilidade e a imagem da Ambidata Group no mercado.

A segurança dos sistemas de informação é cada vez mais colocada à prova por diversos tipos de ameaças, onde se incluem:

- Fraudes eletrónicas e ataques de engenharia social;
- Fuga ou divulgação não autorizada de informação
- Acesso não autorizado a código fonte e propriedade intelectual;
- Ransomware e outras formas de software malicioso;
- Indisponibilidade de serviços cloud, incluindo ataques de negação de serviço (DoS/DDoS), mitigados ao nível da infraestrutura dos nossos fornecedores cloud, no âmbito do modelo de responsabilidade partilhada;
- Comprometimento de credenciais de acesso a sistemas e ambientes cloud;
- Erros humanos;
- Causas naturais (ex. inundação).

Assim, é adotado um plano de segurança estratégico global na Ambidata Group, assente numa abordagem inicial ao negócio, identificando vulnerabilidades, avaliando ameaças e dimensionando os investimentos necessários para reduzir o risco a níveis aceitáveis.

4 Estratégia de Segurança da Informação

A estratégia de segurança da Ambidata Group assenta em três pilares fundamentais:

- Políticas de Gestão de Segurança da Informação: alinhadas com o negócio e os processos que o sustentam;
- Recursos humanos: colaboradores que asseguram a implementação e a funcionalidade do sistema;
- Tecnologia: meios e modelos técnicos de suporte aos procedimentos de segurança.

Uma vez identificados os requisitos de segurança, são selecionados e implementados controlos adequados para garantir que os riscos são mitigados a um nível considerado aceitável. Os controlos são selecionados com base no custo da implementação, no grau de risco identificado e no impacto potencial de uma perda ou comprometimento de informação.

5 Determinar os Ativos de Informação

Os ativos de informação são inventariados pelo SGSI, considerando não só o ativo em si, mas também os seguintes atributos:

- Responsável pelo ativo;
- Controlo do ativo;
- Informação existente associada;
- Classificação da informação;
- Controlos de proteção aplicados.

A utilização e manuseamento adequado dos ativos de informação está inerente à classificação da informação existente e ao descrito nas respetivas Instruções de Trabalho. A preservação dos ativos e a sua adequação/manutenção são asseguradas pelos respetivos responsáveis.

Todos os colaboradores devolvem os ativos pertencentes à empresa, em sua posse, após o término do seu vínculo contratual.

6 Controlos de Segurança da Informação

Após a avaliação do risco e a identificação das medidas mitigadoras, são selecionados e implementados os controlos apropriados para garantir que o risco é reduzido a um nível aceitável. Os controlos de segurança da informação podem ser selecionados a partir da norma NP EN ISO/IEC 27001 (Anexo A) ou de outros conjuntos de controlos, podendo ser adicionados controlos adicionais para responder a necessidades específicas.

A seleção dos controlos baseia-se nas decisões da Ambidata Group., tendo em conta:

- Critérios de aceitação do risco;
- Opções de tratamento do risco;
- Regulamentação e legislação nacional e europeia aplicável, designadamente o RGPD.

Os mecanismos de segurança implementados são alvo de revisões periódicas para garantir os níveis de segurança esperados, com particular enfoque na salvaguarda da continuidade do negócio e dos processos críticos.

7 Responsabilidades

Remissão para o Sistema de Gestão da Qualidade
A estrutura organizacional da Ambidata Group., incluindo o organograma completo e a descrição dos departamentos, encontra-se documentada no **Manual de Gestão** (elaborado no âmbito da certificação NP EN ISO 9001). O presente documento deve ser lido em conjunto com esse manual.
Referência do documento: *M_QLD_046_AMB_Manual de Gestão*

Os papéis e responsabilidades específicos do SGSI, que complementam a estrutura organizacional existente, são os seguintes:

Papel / Função
Administração
Gestor do SGSI
ASI — Ambidata Security & IT Infrastructures
Gestor de SI
Todos os colaboradores

A Política de Segurança da Informação destina-se a todas as partes interessadas da Ambidata Group, independentemente do seu vínculo (colaboradores, fornecedores, consultores, temporários, etc.). Os intervenientes que deliberadamente violem esta ou outras políticas podem ser sujeitos a sanções disciplinares ou outras previstas na lei.

8 Definições

SGSI	Sistema de Gestão de Segurança da Informação.
SGI	Sistema de Gestão Integrado (engloba SGSI e SGQ).
Risco	Efeito da incerteza nos objetivos (ISO 31000 e ISO 27005)
Ameaça	Origem ou causa potencial de um incidente indesejado que pode resultar num dano para a organização ou para os seus ativos.
Vulnerabilidade	Fraqueza de um ativo que pode ser explorada por uma ameaça.
Controlo	Medida implementada para modificar ou mitigar um risco.
Incidente de SI	Evento ou conjunto de eventos indesejáveis de segurança da informação com probabilidade significativa de comprometer as operações de negócio.
ASI	Ambidata Security & IT Infrastructures — equipa interna responsável pela segurança operacional e infraestrutura tecnológica.
Dados pessoais	Informação relativa a uma pessoa singular identificada ou identificável (RGPD, Artigo 4.º).
RGPD	Regulamento Geral sobre a Proteção de Dados (Regulamento (UE) 2016/679).

9 Documentos Associados

- Declaração de Aplicabilidade (SoA)
- Matriz de Risco
- Inventário de Ativos de Informação
- Instruções de Trabalho
- Manual de Gestão
- Políticas específicas de segurança da informação

10 Revisão da Política de Segurança

A presente política de segurança da informação deverá ser revista anualmente ou sempre que ocorram alterações significativas na organização, no contexto de negócio, na legislação aplicável ou na ocorrência de incidentes de segurança relevantes.

11 Referências Normativas

- NP EN ISO/IEC 27001
- ISO/IEC 27002
- Regulamento (UE) 2016/679 — Regulamento Geral sobre a Proteção de Dados (RGPD).