CYBERSECUR - CONSULTORIA E SEGURANÇA DE SISTEMAS LDA

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Código:	SGSI-POL-01-23-1.0
Versão:	1.0
Data da Versão:	30/10/2023
Autor:	Integrity e CyberSecur
Aprovado por:	Direcção Geral
Classificação:	INTERNO

Histórico de Alterações

Data	Versão	Autor	Descrição da Alteração
11/05/2023	0.1	Integrity e CyberSecur	Criação do template do documento do âmbito
18/07/2023	0.2	Integrity	Fomatação de documento
08/08/2023	0.3	Integrity	Fomatação de documento
30/10/2023	1.0	Cybersecur	Aprovação do documento

Índice

1. Objectivos

Esta política de alto nível define a finalidade, a direcção, os princípios e as regras fundamentais da gestão de segurança da informação, segundo as características e necessidades do negócio da CyberSecur e das suas partes interessadas.

2. Âmbito do Documento

A política de segurança da informação é aplicada ao âmbito definido pelo Documento de Âmbito do Sistema de Gestão da Segurança da Informação (doravante designado de SGSI).

3. Destinatários

Este documento é destinado a todos os colaboradores, prestadores de serviços, fornecedores e partes interessadas da CyberSecur, abrangidos pelo âmbito do SGSI, que tenham acesso, direito de uso ou controlo sobre activos de informação da organização e/ou aos recursos a eles associados.

4. Documentos de Referência

ISO/IEC 27001 *Information technology – Security techniques – Information security management systems – Requirements*, cláusula 5.2 e controlo A.5.1.1

ISO/IEC 27000 *Information technology – Security techniques – Information security management systems – Overview and vocabulary*

5. Política de Segurança da Informação

A CyberSecur compromete-se, através da presente política e dos objectivos adiante explicitados, a garantir a segurança da sua informação, assim como a segurança de todos os recursos a ela associados, sejam eles processuais, tecnológicos ou humanos. A proteção da informação é fundamental para o sucesso estratégico da organização e para a sustentabilidade do negócio. Com esse propósito a CyberSecur estabeleceu um SGSI que dispõe de todas as ferramentas necessárias para a gestão segura da informação e dos sistemas de suporte, e que assegura, através de uma abordagem baseada na gestão de risco e na melhoria contínua, a confidencialidade, a integridade e a disponibilidade da informação. As salvaguardas destes três pilares da segurança da informação constituem um garante da imagem, reputação e credibilidade da organização e dos seus processos produtivos junto aos parceiros e clientes.

A CyberSecur subscreve os princípios preconizados no referencial ISO/IEC 27001 e compromete-se a:

a) Assegurar o estabelecimento e a prossecução dos princípios descritos nesta política, bem como a sua aprovação, publicação e comunicação a todos os colabores e entidades externas relevantes;
b) Garantir todos os recursos necessários para a operacionalização dos processos e actividades de gestão da segurança da informação, nomeadamente no que respeita à sensibilização e consciencialização de colaboradores internos e externos para com a temática e para com o seu papel na eficácia do SGSI;
c) Assegurar a definição, implementação e revisão da estratégia de gestão de segurança da informação e garantir o correcto alinhamento com as políticas e objectivos estratégicos de negócio da CyberSecur;
d) Assegurar que o SGSI atinge os resultados pretendidos;
e) Promover de forma estruturada e sistemática a melhoria contínua.

5.1 Objectivos de Segurança da Informação

A CyberSecur estabelece os seguintes objectivos de segurança da informação:

a) Garantir a conformidade com os requisitos legais e regulamentares aplicáveis ao negócio e previstos na legislação nacional;
b) Garantir a integração de prácticas e operações de gestão da segurança da informação em funções e processos de negócio;
c) Assegurar a disponibilidade, integridade e confidencialidade da informação, dos serviços e das infraestruturas, quer em circunstâncias normais de funcionamento quer em circunstâncias excecionais;
d) Garantir que as medidas de segurança do SGSI são compreensíveis, eficazes e com uma adequada relação de custo/benefício;
e) Garantir que o acesso aos sistemas de informação obedece aos princípios de identificação, autenticação, autorização, não-repúdio e auditabilidade;
f) Prever a existência de processos de monitorização que garantam a correcta implementação dos controlos de segurança nas normas e procedimentos da Instituição.

A não aplicação dos princípios e objectivos previstos nesta política por parte de colaboradores, internos ou externos, e entidades prestadoras de serviços, configuram uma violação susceptível de acção disciplinar ou criminal.

A CyberSecur procede à revisão dos objectivos de segurança da informação em intervalos regulares de modo a assegurar a sua contínua pertinência, adequação e eficácia.

6. Matriz de Responsabilidades (RACI)

Actividade	**Gestão de Topo**	**Comité de Segurança da Informação**	**Gestor de Segurança da Informação**	**Trabalhadores e Partes Interessadas**
Elaboração	A	R	C	I
Aprovação	A	C	I	I
Comunicação	A	R	I	I
Revisão	A	R	I	I

Legenda:

Responsabilidade (R):	Responsável por executar a actividade, o executante.
Autoridade (A):	Responsável pela actividade, o dono.
Consultado (C):	Quem deve ser consultado e participar na decisão/actividade no momento em que for executada.
Informado (I):	Quem deve receber a informação de que a actividade foi executada.

7. Documentos Associados

SGSI-DOC-01-Âmbito do SGSI

8. Definições e Acrónimos

Consultar glossário do SGSI.