SECURNET

ALWAYS ONLINE | ALWAYS SECURE

Política de Segurança da Informação

INFORMAÇÃO PÚBLICA

(SGSI)

Sistema de Gestão de Segurança de Informação

PROPRIEDADE E DIVULGAÇÃO

A RELOAD - Consultoria Informática, Unipessoal, Lda possuí a marca comercial registada SECURNET, sob a qual se apresenta globalmente no mercado, sendo por isso assim doravante denominada neste documento. Estas informações devem ser utilizadas de acordo com a classificação atribuída ao documento. A divulgação, reprodução ou uso não autorizado das informações contidas neste documento é proibida.

INFORMAÇÃO DO DOCUMENTO

Título	Política de Segurança da Informação
Âmbito	☒ Sistema de Gestão da Segurança da Informação
Versão	2.1
Referência	SGSI-POL.001
Classificação da Informação	PÚBLICA
Dono do Documento	ISO

CONTROLO DOCUMENTAL

Versão	Data	Autor	Aprovado por	Descrição
2.1	24.09.2025	Equipa de Consulting	CEO	Colocação do documento em novo template aprovado
2.0	22.09.2025	Equipa de Consulting	CEO	Adequação do documento (POL.020.01 - Política de Topo de Segurança de Informação) aos requisitos do SGSI
1.1	06.04.2024	Equipa de Segurança	CISO	Criação da POL.020.01 Política de Topo de Segurança de Informação e atualização da Política de Segurança
1.0	27.03.2023	Equipa de Segurança	CISO	Criação da Política de Segurança SECURNET

ÍNDICE

1. ÂMBITO

A SECURNET reconhece a informação como um ativo estratégico fundamental para a sua atividade, atribuindo-lhe a máxima prioridade e promovendo uma cultura de responsabilidade partilhada e transversal na sua proteção e gestão diária.

A informação é um bem tão importante como qualquer outro bem da organização, pelo que tem de ser protegida da forma mais apropriada. Esta abordagem permite garantir a continuidade do negócio, mitigar riscos relevantes e maximizar o desempenho operacional e a qualidade dos serviços prestados.

Esta política aplica-se, obrigatoriamente, a:

i) Todos os colaboradores da SECURNET, independentemente do seu vínculo contratual;

ii) Todas as entidades externas que, de forma direta ou indireta, acedam, processem ou manuseiem informação sob a responsabilidade da SECURNET.

O não cumprimento desta política, seja de forma intencional ou por negligência, poderá resultar na instauração de processos disciplinares, sancionatórios ou legais, conforme previsto na legislação em vigor e nos normativos internos aplicáveis.

2. OBJETIVO

A Política de Segurança de Informação da SECURNET estabelece os princípios e requisitos fundamentais para a proteção da informação, independentemente do seu formato, suporte, estado (em trânsito, em repouso ou em uso), no contexto das atividades desenvolvidas pela organização.

Esta política visa assegurar a proteção da informação contra perdas de confidencialidade, integridade, disponibilidade, autenticidade, não repúdio, privacidade e propriedade, através da gestão adequada dos riscos e da implementação de controlos técnicos, organizacionais e humanos eficazes.

Através da aplicação desta política, a SECURNET compromete-se a atingir os seguintes objetivos:

- Reforçar a segurança e a resiliência dos sistemas de informação e das equipas que os operam;
- Assegurar uma resposta integrada e eficaz à segurança da informação nos serviços prestados aos clientes e na operação interna;
- Melhorar continuamente a capacidade de resposta e recuperação face a incidentes de segurança;
- Garantir a conformidade com os requisitos legais, normativos e contratuais, incluindo regulamentos nacionais e internacionais relevantes;
- Otimizar custos não planeados associados a falhas de segurança, incidentes ou interrupções de serviço, através da prevenção e mitigação eficazes.

3. POLÍTICA

A SECURNET presta serviços nas áreas da segurança de dados orientados a infraestruturas de IT, com a missão de colocar organizações "*Always online, Always Secure*", tem como princípios garantir os níveis adequados de integridade, autenticidade, disponibilidade e confidencialidade, requeridos para a sua proteção da informação da organização e dos seus clientes.

3.1. Compromisso e Princípios da Segurança da Informação

Em conformidade com a legislação e normativos em vigor, a SECURNET, através da sua Gestão de Topo, compromete-se com a segurança da informação, adotando as melhores práticas nacionais e internacionais, na perspetiva de garantir os princípios fundamentais de segurança da informação:

- Garantir a existência de mecanismos que assegurem, na medida do razoável, a confidencialidade, integridade, disponibilidade, autenticidade, não-Repúdio, privacidade e propriedade da Informação;
- Assegurar uma gestão de risco continua para avaliar a exposição ao risco dos ativos de informação, gerir e tratar esses riscos em cumprimento com a tolerância ao risco definida pela organização;
- Garantir que todos os incidentes de segurança da informação e violações de dados pessoais, reais ou suspeitas, sejam prontamente

investigados, tratados, relatados internamente e à autoridade supervisora competente, quando aplicável;

- Planear e promover a formação e consciencialização dos colaboradores e entidades externas de acordo com as suas funções e responsabilidades, bem como das atividades e iniciativas previstas garantindo por parte dos colaboradores e entidades externas o compromisso de cumprimento da presente política;
- Garantir que as entidades externas com acesso à informação da SECURNET, ou de clientes, se encontram a par das suas responsabilidades ao nível da Segurança da Informação;
- Garantir Planos de Continuidade dos processos críticos e das operações da SECURNET em cenários de incidentes disruptivos, de forma a salvaguardar os compromissos assumidos com os clientes;
- Cumprir com as suas obrigações contratuais e legais relativamente à Segurança da Informação e proteção de dados pessoais;
- Definir claramente as responsabilidades de segurança da informação, garantindo que todos entendem as suas funções específicas. As pessoas com autoridade devem assegurar e comprovar a conformidade com a Política de Segurança da Informação, através de evidências e documentação verificáveis;
- Promover a melhoria continua dos processos e controlos de segurança da informação tendo como referência orientadora os regulamentos, normas e boas praticas aplicáveis;
- Assegurar a existência de mecanismos de comunicação de eventos de segurança por parte dos intervenientes no sistema e procedimentos para a sua deteção, análise, resposta e resolução;
- Assegurar a existência de mecanismos de controlo de acessos para garantir que o acesso à informação é concebido sob o princípio do acesso mínimo;
- Realizar a monitorização e avaliação do Sistema de Gestão de Segurança da Informação de forma a assegurar o cumprimento dos objetivos definidos, bem como realizar as revisões de gestão que potenciem a sua contínua melhoria, adequação e eficácia;

- Envolver, consciencializar, informar e promover a colaboração e comunicação eficaz entre as diferentes partes interessadas sobre as questões da segurança da informação para garantir que estes mantêm padrões de segurança compatíveis com os da SECURNET.

4. REQUISTOS LEGAIS E OUTROS APLICÁVEIS

A presente política evidência o compromisso da gestão de topo da SECURNET, e traduz o compromisso de toda a Organização com a segurança de informação, no contexto do seu Sistema de Gestão de Segurança de Informação (SGSI), estabelecendo os princípios orientadores que regem a proteção da informação em todas as suas formas, suportes e ciclos de vida.

O SGSI da SECURNET está alinhado com as melhores práticas nacionais e internacionais, e encontra-se em conformidade com:

- O Regime Jurídico da Segurança do Ciberespaço (Lei n.º 59/2025)
- O Regulamento Geral sobre a Proteção de Dados (RGPD);
- A norma ISO/IEC 27001:2022;
- A norma portuguesa DNP TS 4475-1:2021;
- Os requisitos internos da organização;
- E, os compromissos assumidos perante as partes interessadas.

5. VIGÊNCIA E REVISÃO

A política entra em vigor na data da sua aprovação, sendo objeto de revisão anual ou sempre que se verifiquem alterações significativas no sentido de providenciar uma melhoria da aplicabilidade, da adequabilidade e da eficácia. Uma vez aprovada a política será comunicada às partes interessadas.

Após a comunicação, a política torna-se instituída, sendo publicada e disponibilizada às partes interessadas nos canais definidos para o efeito.