CMORE

Beyond the Obvious

Política de Segurança da Informação

1 | PROPÓSITO |

Este documento define a política de segurança da informação da C-MORE Sustainability, a seguir designada por C-MORE.

Esta Política visa definir o propósito, direção, princípios e regras básicas para a Gestão da Segurança da Informação. A C-MORE gere os seus Sistemas de Segurança da Informação utilizando as melhores práticas internacionais, seguindo as normas ISO/IEC 27001:2022.

A C-MORE implementou um conjunto de controlos de segurança da informação para fazer face aos seus riscos percecionados e garantir que as operações funcionam de forma adequada e sem interrupções em benefício dos seus clientes, acionistas e outras partes interessadas.

Os controlos selecionados e o seu status de implementação estão enumerados na Declaração de Aplicabilidade da Empresa.

2 | ÂMBITO |

Esta política aplica-se a todos os sistemas, pessoas e processos da Organização, que constituem o Sistema de Gestão da Segurança da Informação para a proteção dos ativos de informação que suportam a conceção, o desenvolvimento, gestão e manutenção da plataforma de ESG *Maturity*, de acordo com a declaração de aplicabilidade "ISMS C-MORE 27001SOA".

3 | O SISTEMA DE GESTÃO DA SEGURANÇA DA INFORMAÇÃO DA C-MORE |

A segurança da informação deve ser apoiada por um sistema de gestão: SGSI – Sistema de Gestão da Segurança da Informação, que inclui um conjunto de políticas e procedimentos que garantem os princípios essenciais da informação: disponibilidade, integridade e confidencialidade, de acordo com os requisitos, leis e regulamentos relevantes do negócio.

3.1 Políticas e Procedimentos SGSI

Todas as políticas e procedimentos que compõem o Sistema de Gestão de Segurança da Informação da C-MORE estão descritos no documento "0. ISMS C-MORE Document list and applicability".

4 | OBJETIVOS E PRINCÍPIOS DE SEGURANÇA DA INFORMAÇÃO |

Dada a importância dos Sistemas de Segurança da Informação, a C-MORE determina os seguintes princípios fundamentais de segurança da informação:

PRINCÍPIOS FUNDAMENTAIS DA SEGURANÇA DA INFORMAÇÃO da C-MORE	
Princípio do cumprimento regulamentar	Todos os Sistemas de Informação devem ser ajustados às normas de aplicação jurídica regulamentar e sectorial que afetam a segurança da informação, especialmente as relacionadas com a proteção de dados pessoais e a segurança dos sistemas.
Princípio da gestão de risco	Os riscos devem ser minimizados para níveis aceitáveis. Os objetivos de segurança devem ser estabelecidos, revistos e coerentes com os aspetos da segurança da informação.
Princípio da sensibilização e formação	Serão realizados programas de formação e campanhas de sensibilização sobre segurança da informação destinados a todos os utilizadores com acesso à informação.
Princípios de confidencialidade, integridade e disponibilidade	+ **Confidencialidade:** Assegurar que apenas utilizadores/sistemas autorizados podem visualizar, aceder, alterar ou utilizar os dados de outra forma. + **Integridade:** Manter a consistência, precisão e confiabilidade dos dados ao longo de todo o seu ciclo de vida. Os dados não devem ser alterados em circulação ou alterados por pessoas não autorizadas. + **Disponibilidade:** As informações devem estar sempre disponíveis para as partes autorizadas. Isto envolve a manutenção adequada de hardware e infraestruturas técnicas e sistemas que detêm e exibem a informação.
Princípio da responsabilidade	Os colaboradores da C-MORE devem ser responsáveis na sua conduta relativamente à segurança da informação, cumprindo com as normas e controlos estabelecidos.
Princípio da melhoria contínua	O grau de eficácia dos controlos de segurança implementados deve ser revisto regularmente para aumentar a capacidade de adaptação à constante evolução do risco e do ambiente tecnológico.

Esta política é o quadro de referência para o estabelecimento dos objetivos de segurança.

5 | REQUISITOS DE SEGURANÇA DA INFORMAÇÃO |

Esta Política e todo o SGSI devem estar em conformidade com os requisitos legais e regulamentares relevantes para a organização no domínio da segurança da informação, bem como com as obrigações contratuais

Alguns dos documentos de referência são:

+ Normas ISO/IEC 27001:2022
+ Declaração de Aplicabilidade
+ RGPD

6 | AVALIAÇÃO DOS PRINCÍPIOS E OBJETIVOS |

Todos os objetivos e princípios são revistos anualmente, assim como as políticas e procedimentos que compõem o Sistema de Gestão da Segurança da Informação da Empresa. Esta revisão pode ter lugar mais cedo quando ocorrerem alterações significativas.

Se esta revisão revelar que é necessário um ajustamento ou alteração de conteúdo, a edição dos documentos deve ser registada no controlo de revisão documental.

As políticas e procedimentos que compõem o sistema de gestão da segurança da informação serão monitorizados no documento de Monitorização da Segurança da Informação e quando se entender que não são eficazes ou que não estão a ser cumpridos, devem ser discutidas formas de assegurar o seu cumprimento.

Se necessário, o Plano de Ação da empresa incluído no Asset Inventory da C-MORE deve ser atualizado, seguindo novos objetivos ou princípios relacionados com a gestão dos sistemas de segurança da informação.

6.1 Melhoria Contínua da Segurança da Informação

A Empresa compromete-se a melhorar continuamente o seu Sistema de Segurança da Informação, tentando:

- Melhorar continuamente a eficácia dos controlos de segurança da informação
- Melhorar os processos atuais para os alinhar com as boas práticas definidas dentro das normas relevantes
- Rever as métricas relevantes numa base anual para avaliar se é apropriado alterá-las, com base em dados históricos recolhidos
- Obter ideias para melhorar através de reuniões regulares e outras formas de comunicação com as partes interessadas
- Rever ideias para melhorias em reuniões regulares de gestão para priorizar e avaliar calendários e benefícios

Ideias para melhorias podem ser obtidas de qualquer fonte incluindo colaboradores, clientes, fornecedores, pessoal de TI, avaliações de risco, e relatórios de serviços. Uma vez identificadas, serão registadas e avaliadas como parte das revisões de gestão.

7 | Documentos Referenciados |

- Políticas e Procedimentos ISMS da C-MORE
- Aplicabilidade do Controlo – Declaração de Aplicabilidade
- Monitorização da Segurança da Informação (ver *Balanced Score Card* da C-MORE)
- Formulário de Gestão de Ativos da C-MORE – Plano de Ação