

cybersafe

Política de Segurança da Informação (Versão Pública)

Classificação: PÚBLICA

cybersafe

Índice

Descrição e controlo do documento **3**

Termo de Responsabilidade 3

Necessidade de Conhecer 3

1. Objetivo **4**

2. Âmbito **4**

3. Princípios de Segurança da Informação **4**

4. Compromissos de Segurança da Informação **4**

5. Sistema de Gestão da Segurança da Informação e Certificação ISO/IEC 27001:2022 ..... **5**

6. Gestão de Incidentes, Continuidade e Resiliência **5**

7. Responsabilidade e Cultura de Segurança **5**

8. Conformidade, Monitorização e Revisão **6**

DESCRIÇÃO E CONTROLO DO DOCUMENTO

Termo de Responsabilidade

Este documento e todo o seu conteúdo constituem propriedade intelectual da CyberSafe, Lda. (doravante CyberSafe), e encontra-se protegido nos termos do Decreto-Lei n.º 63/85, de 14 de março – Código do Direito de Autor e dos Direitos Conexos. A divulgação, transcrição ou reprodução desta política não é permitida sem autorização prévia, por escrito, da CyberSafe, Lda.

O destinatário do documento compromete-se a utilizar a aludida informação exclusivamente com a finalidade de apreciação do mesmo, tendo em conta o respetivo âmbito. A utilização de toda ou parte da informação contida no presente documento para outros fins que não os definidos no seu âmbito, deverá ser previamente autorizada pela CyberSafe.

Os documentos classificados como "PRIVADO" ou "INTERNO" incluem informações que não são do domínio público e não devem estar acessíveis ao público em geral. A sua consulta está autorizada apenas às entidades definidas na secção "Necessidade de Conhecer". O leitor compromete-se a não revelar, duplicar ou disponibilizar quaisquer informações neles contidas a quaisquer terceiros.

Os documentos classificados, devidamente marcados com as designações "MUITO SECRETO", "SECRETO", "CONFIDENCIAL", "RESERVADO", são apenas distribuídos por via segura a indivíduos ou entidades com a respetiva credenciação de segurança, atribuída pelo Gabinete Nacional de Segurança (GNS) — nomeadamente Credenciação de Pessoa ou Credenciação de Pessoa Coletiva, conforme aplicável.

Classificação do Documento

PÚBLICO

Âmbito do Documento

Política Pública

Necessidade de Conhecer

- CyberSafe
- Público em geral

Controlo de versões

VERSÃO	DATA	AUTOR	DETALHES	APROVADOR	DATA APROVAÇÃO
1.0	15/09/2026	CyberSafe	Desenvolvimento do Política de Segurança da Informação – Versão Pública		

1. Objetivo

A CyberSafe considera a informação um ativo essencial para o desenvolvimento da sua atividade e, como tal, assume o compromisso de a proteger de forma adequada, responsável e proporcional aos riscos a que se encontra exposta.

Esta Política de Segurança da Informação define os princípios e compromissos que orientam a CyberSafe na proteção da informação, procurando garantir a sua confidencialidade, integridade e disponibilidade. A sua aplicação visa proteger os ativos da organização, assegurar a continuidade das atividades e dos serviços e reforçar a confiança dos clientes, parceiros, fornecedores e demais partes interessadas.

A CyberSafe compromete-se ainda a cumprir os requisitos legais, regulamentares e contratuais aplicáveis à sua atividade, bem como a manter e melhorar continuamente o seu Sistema de Gestão da Segurança da Informação (SGSI).

2. Âmbito

Esta Política aplica-se à informação tratada pela CyberSafe no âmbito das suas atividades, independentemente do seu formato, suporte ou localização.

Os princípios estabelecidos nesta Política abrangem os colaboradores, prestadores de serviços, parceiros, fornecedores e outras partes interessadas que, no âmbito da sua relação com a CyberSafe, tenham acesso à informação, aos sistemas ou aos recursos que a suportam.

A aplicação desta Política é realizada de forma proporcional à natureza da informação, aos riscos associados e aos requisitos legais, regulamentares e contratuais aplicáveis.

3. Princípios de Segurança da Informação

A abordagem da Cybersafe à Segurança da Informação rege-se pelos seguintes princípios:

Confidencialidade — Assegurar que a informação apenas é disponibilizada ou divulgada a pessoas, entidades ou processos devidamente autorizados.

Integridade — Preservar a exatidão e completude da informação, protegendo-a contra alterações indevidas ou não autorizadas.

Disponibilidade — Assegurar que a informação e os recursos necessários estão acessíveis e utilizáveis pelas partes autorizadas quando necessário.

Gestão de Risco — Identificar, avaliar e tratar os riscos de Segurança da Informação de forma sistemática e proporcional à criticidade dos ativos, processos e serviços.

Responsabilidade Partilhada — Promover a participação e responsabilização de todos os intervenientes na proteção da informação.

Melhoria Contínua — Monitorizar, avaliar e melhorar continuamente as práticas e os controlos de Segurança da Informação, considerando a evolução dos riscos, das tecnologias, do negócio e dos requisitos aplicáveis.

4. Compromissos de Segurança da Informação

No âmbito do seu Sistema de Gestão da Segurança da Informação, a CyberSafe compromete-se a:

- Proteger a confidencialidade, integridade e disponibilidade da informação sob a sua responsabilidade;

- Implementar e manter controlos técnicos e organizacionais adequados aos riscos identificados;
- Proteger a informação contra acesso não autorizado, alteração, perda, destruição ou divulgação indevida;
- Gerir os acessos à informação de acordo com as necessidades, funções e responsabilidades aplicáveis;
- Identificar, avaliar e tratar os riscos de segurança da informação;
- Classificar e proteger a informação de acordo com a sua sensibilidade, valor, criticidade e requisitos aplicáveis;
- Considerar os requisitos de segurança da informação na gestão de sistemas, serviços, processos e respetivas alterações;
- Promover a formação e sensibilização contínua dos colaboradores e demais partes relevantes;
- Considerar os requisitos de segurança da informação nas relações com clientes, fornecedores, parceiros e outros terceiros;
- Adotar medidas de continuidade e recuperação adequadas à criticidade dos processos e serviços;
- Monitorizar e avaliar regularmente a eficácia dos controlos e medidas de segurança implementados;
- Assegurar o cumprimento dos requisitos legais, regulamentares e contratuais aplicáveis;
- Promover a melhoria contínua do sistema de gestão da segurança da informação.

5. Sistema de Gestão da Segurança da Informação e Certificação ISO/IEC 27001:2022

A CyberSafe mantém um Sistema de Gestão da Segurança da Informação (SGSI) através do qual estabelece uma abordagem estruturada e baseada no risco para a proteção da informação, gestão dos controlos de segurança e melhoria contínua.

No âmbito do seu compromisso com a Segurança da Informação, o SGSI da Cybersafe é certificado de acordo com a norma ISO/IEC 27001:2022, no âmbito da prestação de serviços de monitorização, deteção, análise e resposta a incidentes de cibersegurança, fornecidos através dos serviços de Security Operations Center (SOC as a Service) e Managed Detection and Response (MDR).

Esta certificação reforça o compromisso da CyberSafe com a adoção de práticas reconhecidas internacionalmente para a gestão da Segurança da Informação, gestão de riscos e melhoria contínua dos processos abrangidos pelo âmbito certificado.

6. Gestão de Incidentes, Continuidade e Resiliência

A CyberSafe mantém processos destinados à identificação, registo, análise e tratamento de eventos e incidentes de Segurança da Informação.

Os incidentes identificados são avaliados de acordo com a sua natureza e impacto, sendo adotadas as medidas de contenção, correção e recuperação consideradas adequadas. Sempre que legal ou contratualmente exigido, são efetuadas as comunicações necessárias às autoridades competentes, clientes ou outras partes interessadas relevantes.

A CyberSafe mantém igualmente medidas de continuidade e resiliência adequadas à criticidade dos seus processos e serviços, com o objetivo de reduzir o impacto de situações adversas e apoiar a continuidade e recuperação das suas atividades.

7. Responsabilidade e Cultura de Segurança

A Segurança da Informação é uma responsabilidade partilhada por todos os que tratam ou têm acesso à informação da CyberSafe.

A Gestão de Topo assegura o apoio à implementação, manutenção e melhoria contínua desta Política e do Sistema de Gestão da Segurança da Informação.

A CyberSafe promove ações regulares de formação e sensibilização, incentivando a adoção de boas práticas, comportamentos responsáveis e a comunicação de eventos ou situações suscetíveis de comprometer a Segurança da Informação.

Todos os colaboradores e terceiros abrangidos por esta Política devem cumprir os princípios, políticas, normas e procedimentos de segurança aplicáveis às atividades que desempenham.

8. Conformidade, Monitorização e Revisão

A Cybersafe compromete-se a cumprir os requisitos legais, regulamentares e contratuais aplicáveis à Segurança da Informação e à proteção da informação sob a sua responsabilidade.

A implementação e a eficácia dos controlos de Segurança da Informação são acompanhadas através de mecanismos adequados de monitorização e auditoria. Os resultados destas atividades, bem como a evolução dos riscos, das ameaças, das tecnologias e dos requisitos aplicáveis, são considerados na melhoria contínua do SGSI.

A presente Política é aprovada pela Gestão de Topo e revista anualmente, ou sempre que ocorram alterações significativas nos ativos de informação, riscos, processos ou requisitos aplicáveis.

As atualizações entram em vigor após a respetiva aprovação e publicação, substituindo as versões anteriores.

Classificação: Pública

Versão: 1.0

Última atualização: Setembro/2026



Alfrapark - Estrada de Alfragide
67 | Edifício H, piso 1 | 2610-008
Alfragide, Portugal

+351 210 360 276
contato@cybersafe.pt