Misericórdia de Cascais
dignidade para todos

Política de Segurança da Informação e CIBERSEGURANÇA

Rui M. F. de Oliveira
Responsável de Cibersegurança

Índice

1. OBJETIVO DA POLÍTICA 3
2. ÂMBITO DE PROTEÇÃO PARA A SEGURANÇA DA INFORMAÇÃO E CIBERSEGURANÇA 3
3. PARTES INTERESSADAS 3
4. COMPROMISSOS PARA A SEGURANÇA DA INFORMAÇÃO E CIBERSEGURANÇA 4
5. PLANO DE SEGURANÇA 4
6. GESTÃO DO RISCO 5
7. INTEGRAÇÃO COM A GESTÃO DA PRIVACIDADE DE DADOS PESSOAIS 5
8. CIBERSEGURANÇA 5
9. GESTÃO DE INCIDENTES 6
10. FUNÇÕES E RESPONSABILIDADES 6
11. PLANO DE SENSIBILIZAÇÃO, FORMAÇÃO E TREINO 8
13. DIVULGAÇÃO E PUBLICAÇÃO 8
14. REGISTO DE REVISÃO 9

1. OBJETIVO DA POLÍTICA

A Misericórdia de Cascais, reconhece como um recurso essencial, indispensável e de alta relevância para a execução eficaz dos serviços oferecidos à comunidade, no cumprimento de suas atribuições.

A Misericórdia de Cascais considera imprescindível estabelecer e implementar uma política que determine os seus compromissos com a proteção dessa informação, nomeando, para isso, um responsável encarregado da gestão da segurança da informação e da respetiva Cibersegurança.

O Responsável pela Cibersegurança deve assegurar que esta política permanece alinhada com os objetivos estratégicos da Misericórdia de Cascais e que está devidamente incorporada no correspondente Plano de Segurança.

A Misericórdia de Cascais assume o compromisso de fornecer os recursos e meios indispensáveis, além de se dedicar à missão de promover a melhoria contínua desses compromissos e das respetivas métricas de eficácia, garantindo, assim, a conformidade com os requisitos legais, bem como com as expectativas e necessidades de segurança identificadas.

2. ÂMBITO DE PROTEÇÃO PARA A SEGURANÇA DA INFORMAÇÃO E CIBERSEGURANÇA

O escopo de proteção para a Segurança da Informação e a correspondente Cibersegurança abrange os serviços essenciais da Misericórdia de Cascais, bem como os ativos e recursos que viabilizam a sua utilização pelas partes interessadas.

Este escopo contempla os fluxos de informação crítica, incluindo a coleta de dados, seu processamento, armazenamento, compartilhamento com as partes envolvidas e a eliminação segura desses dados.

3. PARTES INTERESSADAS

Consideram-se como partes interessadas todas as pessoas, organizações públicas ou privadas que estabelecem interação com o escopo de proteção da Segurança da Informação e Cibersegurança.

No contexto da presente política, identificam-se:

- **Partes interessadas internas** – Corpos Sociais, trabalhadores detentores dos vários vínculos laborais previstos na Lei Geral do Trabalho para IPSS.

- **Partes interessadas externas** – Administração Pública Central de tutela às IPSS; Entidades reguladoras – Centro Nacional de Cibersegurança; Comissão Nacional de Proteção de Dados; ERS - Entidade Reguladora da Saúde; SPMS – Serviços Partilhados do Ministério da Saúde; ULS de Lisboa Ocidental; Ministério da Educação; Munícipes; Agrupamentos escolares do concelho de Cascais; Juntas de freguesia do Concelho de Cascais e Oeiras; Câmara Municipal de Cascais e de Oeiras, Pessoas singulares ou entidades com interesses no âmbito da geografia da

intervenção da Misericórdia de Cascais; União das Misericórdias Portuguesas; Associações sem fins lucrativos do concelho de Cascais e Oeiras; Instituições privadas de solidariedade social do concelho de Cascais e Oeiras; Prestadores de Serviços/Avençados; Prestadores de Serviços/fornecedores.

Para cada caso, serão analisados os requisitos de segurança que constam em legislação, regulamentação, contratos, protocolos ou outros compromissos firmados com a Misericórdia de Cascais.

4. COMPROMISSOS PARA A SEGURANÇA DA INFORMAÇÃO E CIBERSEGURANÇA

A Misericórdia de Cascais acompanha os desenvolvimentos legislativos nacionais e europeus, buscando, por meio desta Política, assegurar o compromisso com a proteção de informações classificadas como críticas para seus serviços essenciais, incluindo dados pessoais de titulares identificados como partes interessadas. Compromete-se, ainda, a identificar e mitigar os riscos de segurança relacionados à perda, destruição, alteração indevida ou acesso não autorizado, seja de forma acidental ou ilícita.

Esta Política estabelece os compromissos da Misericórdia de Cascais com a Segurança da Informação e Cibersegurança, os quais incluem as seguintes garantias:

- **Confidencialidade –** Garantir que apenas os utilizadores, internos ou externos, devidamente autorizados, tenham acesso à informação;
- **Privacidade –** Garantir que os dados pessoais dos titulares, tratados como informação confidencial, sejam coletados, processados e armazenados exclusivamente com base em fundamentos legais válidos, respeitando os princípios do quadro normativo em vigor;
- **Integridade –** Garantir a proteção da informação contra alterações e/ou destruições não autorizadas, preservando sua exatidão e autenticidade;
- **Disponibilidade –** Garantir que a informação esteja acessível sempre que necessário para a realização de atividades, respeitando a confidencialidade, privacidade e integridade;
- **Irrefutabilidade** – Garantir que todos os utilizadores, enquanto emissores de informações ou ao compartilharem dados pessoais com destinatários autorizados, sejam identificados física e digitalmente com valor probatório legal;
- **Cibersegurança** – Garantir a proteção dos compromissos mencionados acima quando os serviços essenciais e os recursos associados estão expostos ao Ciberespaço e a eventuais Ciberataques.

5. PLANO DE SEGURANÇA

O Plano de Segurança tem como propósito estabelecer, implementar, manter e aprimorar continuamente um conjunto de diretrizes, práticas, controles de segurança, ações de monitorização e auditoria, que assegurem o cumprimento dos compromissos assumidos pela Misericórdia de

Cascais no contexto da proteção da Segurança da Informação.

Para cumprir de forma eficaz os compromissos e objetivos estabelecidos nesta política, serão implementados os seguintes mecanismos de execução:

- Estabelecimento, validação e disseminação de políticas temáticas adicionais para a gestão da Segurança da Informação;
- Fomento de iniciativas de conscientização, capacitação e treinamento dos colaboradores;
- Avaliação e gerenciamento dos riscos identificados, incluindo os respetivos planos de tratamento de riscos e os riscos residuais associados;
- Definição e implementação de medidas de segurança para mitigação dos riscos;
- Administração de incidentes relacionados à segurança da informação e execução de respostas adequadas para assegurar a continuidade dos sistemas de informação nas atividades protegidas;
- Execução de auditorias internas para identificação de áreas de melhoria;
- Atualização do Plano de Segurança e análise de indicadores de desempenho para medir a eficácia.

6. GESTÃO DO RISCO

Reconhecendo-se como uma ferramenta essencial para o alcance dos objetivos do Plano de Segurança e para a execução dos compromissos assumidos nesta política de segurança, serão realizadas análises de risco de forma periódica, com o propósito de adotar medidas de tratamento apropriadas e proporcionais aos níveis de risco detetados.

Os mecanismos de segurança a serem implementados serão definidos com base nos resultados dessas análises, com a finalidade de garantir uma redução eficaz dos riscos e a minimização do risco residual.

7. INTEGRAÇÃO COM A GESTÃO DA PRIVACIDADE DE DADOS PESSOAIS

Ao estabelecer a privacidade como um dos pilares da segurança da informação, a Misericórdia de Cascais promove a aplicação integrada de medidas de segurança que garantam o tratamento adequado dos riscos, em conformidade com os requisitos do Regulamento Geral sobre a Proteção de Dados e demais legislações correlatas, assegurando o cumprimento rigoroso da Política de Privacidade e Gestão de Dados Pessoais da Misericórdia de Cascais.

8. CIBERSEGURANÇA

As informações essenciais para os serviços críticos, bem como os dados pessoais processados internamente pela Misericórdia de Cascais, de acordo com o âmbito de proteção definido, serão devidamente resguardados contra ameaças ou ataques, sejam eles externos ou internos, realizados

por meio de métodos ou mecanismos que possam comprometer a Cibersegurança da Misericórdia de Cascais e de todas as partes que interagem com a instituição.

Para tal, a Cibersegurança é entendida como a garantia de que os compromissos de segurança previstos nesta política são mantidos, mesmo diante de potenciais exposições ao Ciberespaço, com os ativos sujeitos ao risco de sofrerem Ciberataques.

A Misericórdia de Cascais cumprirá as exigências e práticas estabelecidas pelo Regime Jurídico da Segurança do Ciberespaço, adotando boas práticas, ações e controles de segurança adequados, previstos no **QNRCS - Quadro Nacional de Referência para a Cibersegurança**, diretrizes normativas e recomendações da **Agência da União Europeia para a Cibersegurança (ENISA)**. Além disso, implementará os procedimentos necessários para a gestão de incidentes, visando a identificação e o tratamento de ataques ou ameaças.

Adicionalmente, a Misericórdia de Cascais aplicará medidas de prevenção e proteção apropriadas e proporcionais, garantindo o cumprimento das responsabilidades assumidas nesta política.

9. GESTÃO DE INCIDENTES

Um incidente de segurança ocorre quando algum dos compromissos de segurança previstos nesta política é comprometido, ou seja, não pode ser sustentado ou demonstrado.

A Misericórdia de Cascais compromete-se a estabelecer um processo de gestão de incidentes, coordenado pelo Responsável pela Segurança, com o objetivo de mitigar o impacto potencial de um ataque interno ou externo e restaurar o funcionamento dos serviços críticos o mais rapidamente possível.

Reconhecendo sua responsabilidade perante as partes interessadas, esse processo inclui ações de comunicação que asseguram a informação adequada sobre o progresso e o tratamento de qualquer incidente de segurança.

Nesse contexto, destaca-se a inclusão do procedimento de reporte de incidentes de Cibersegurança à entidade nacional responsável, o Centro Nacional de Cibersegurança.

10. FUNÇÕES E RESPONSABILIDADES

Os envolvidos com atribuições e responsabilidades relacionadas à gestão e implementação desta política são os seguintes:

1. Órgão Executivo (Mesa Administrativa)

A Mesa Administrativa garante que esta política e os objetivos de segurança estão definidos e alinhados com a orientação estratégica da Misericórdia de Cascais, assegurando também a incorporação dos requisitos de segurança da informação nos processos organizacionais, além da disponibilização dos recursos indispensáveis para a gestão eficiente do Plano de Segurança. A Mesa Administrativa aprova e delibera, no âmbito de suas atribuições, as ações necessárias para a implementação eficaz do Plano de Segurança da Misericórdia de Cascais.

2. Responsável de Segurança

O Responsável de Segurança é designado pela Senhora Provedora para desempenhar, entre outras, as seguintes atribuições:

a) Garantir a definição e execução das atividades relacionadas à implementação, manutenção e operação da estratégia de Segurança da Informação e Cibersegurança da Misericórdia de Cascais;

b) Assegurar a conformidade com a legislação e regulamentação aplicável, incluindo o Regime Jurídico da Segurança do Ciberespaço e o quadro normativo vigente relacionado à proteção de dados;

c) Conhecer e promover a adoção de boas práticas em Segurança da Informação e Cibersegurança;

d) Supervisionar e validar a avaliação periódica dos riscos de segurança e os correspondentes planos de tratamento;

e) Fomentar a criação e execução de programas de formação, sensibilização e conscientização sobre segurança da informação para os colaboradores da Misericórdia de Cascais;

f) Monitorar e avaliar a gestão de incidentes de segurança e as ações para assegurar a continuidade dos serviços;

g) Coordenar a equipe responsável pela realização das auditorias internas necessárias.

3. Pontos de Contacto Permanente

A Provedora da Misericórdia de Cascais é responsável por nomear o(s) Ponto(s) de Contacto Permanente.

O Ponto de Contacto Permanente tem as seguintes funções:

1) Coordenar com outras entidades a eficácia na resposta a incidentes de segurança que impactem as atividades da Misericórdia de Cascais, sob supervisão do Responsável de Segurança;
2) Implementar os procedimentos estabelecidos no Plano de Segurança da Misericórdia de Cascais;
3) Assegurar a recolha de informação operacional e técnica após a notificação de incidentes relevantes ou substanciais, quer submetidos pela Misericórdia de Cascais, quer por outras entidades cujo sistema de informação possa influenciar as atividades da instituição, incluindo diretrizes técnicas emitidas pelo Centro Nacional de Cibersegurança no âmbito das suas competências;
4) Obter e atualizar dados integrados sobre a situação no contexto de um incidente de impacto significativo;
5) Facilitar a troca de informações em cenários onde sejam ativados planos de emergência de proteção civil relacionados diretamente ou que influenciem a segurança do ciberespaço, bem como em planos associados ao planeamento civil de emergência cibernética ou à segurança de infraestruturas críticas, nacionais ou europeias, com implicações nos sistemas de informação da Misericórdia de Cascais;
6) Executar os procedimentos definidos em planos de emergência de proteção civil quando estes

afetem as redes e sistemas de informação, ou em iniciativas de planeamento civil de emergência do ciberespaço.

4. Pessoas com acesso ao Sistema de Informação

Todos os utilizadores habilitados a aceder ao Sistema de Informação da Misericórdia de Cascais serão conscientizados por meio de ações previstas no plano de formação interna, visando o desempenho das funções associadas à sua categoria profissional, em alinhamento com a missão, os objetivos e as responsabilidades definidos nesta política.

Após a divulgação e publicação desta Política, os utilizadores dos recursos do Sistema de Informação passam a estar vinculados às seguintes obrigações:

- Participar nas ações de capacitação previstas no plano de formação vigente, seja no momento da sua integração na Misericórdia de Cascais, em caso de mudança de funções, ou conforme a periodicidade definida para cada sessão de formação;
- Preservar os ativos informacionais sob sua responsabilidade;
- Contribuir para a gestão de riscos associados aos recursos atribuídos;
- Garantir que os recursos disponibilizados são utilizados exclusivamente para finalidades profissionais;
- Relatar qualquer ocorrência que possa comprometer a segurança da informação;
- Considerar e seguir as orientações/comunicados transmitidos pela Misericórdia de Cascais no âmbito da Segurança da Informação e do Ciberespaço;
- Adotar e assegurar o cumprimento das diretrizes estabelecidas nesta política.

Em caso de violação das diretrizes estabelecidas nesta política, a Misericórdia de Cascais adotará as medidas necessárias para que o responsável seja responsabilizado pelos seus atos, de acordo com os enquadramentos de responsabilidade civil, penal, contraordenacional e/ou disciplinar.

11. PLANO DE SENSIBILIZAÇÃO, FORMAÇÃO E TREINO

A Misericórdia de Cascais promove a execução de um plano periódico de conscientização, capacitação e treinamento dos utilizadores, que contempla a divulgação de boas práticas, ações formativas em formatos “online” e presenciais, além de testes de procedimentos de resposta a incidentes para reforço de treino e preparação.

A eficácia deste plano é assegurada por meio de um conjunto de iniciativas destinadas a garantir a qualificação e prontidão dos utilizadores no âmbito da Segurança da Informação, da Cibersegurança, bem como da Ciberhigiene pessoal, conforme definido no Plano de Segurança.

12. MANUTENÇÃO, MELHORIA CONTÍNUA E REVISÃO

Todas as políticas, diretrizes e demais documentos que sustentam o Plano de Segurança serão

revisados e ajustados sempre que ocorrerem mudanças no contexto ou na estratégia da Misericórdia de Cascais, alterações na lista de partes interessadas e nos seus respetivos requisitos, ou ainda em decorrência de modificações organizacionais significativas nos processos associados ao desempenho das competências atribuídas.

O Responsável de Segurança compromete-se, ainda, a garantir que essa revisão e atualização seja realizada, no mínimo, uma vez por ano.

13. DIVULGAÇÃO E PUBLICAÇÃO

Considerando a classificação atribuída a esta política, o documento será disponibilizado em formato PDF não editável a todas as partes interessadas, por meio dos canais de comunicação digitais da Misericórdia de Cascais.

14. REGISTO DE REVISÃO

VERSÃO	MOTIVO DA REVISÃO	ELABORADO POR	APROVADO POR	DATA APROVAÇÃO
0.1	Criação e redação	Serviço de TI	Responsável de Cibersegurança	**05/12/2024**
1.0	**Aprovação**	**Serviço de TI**	**Mesa Administrativa**	**10/12/2024**