EDITAL

---------- MÁRIO CONSTANTINO ARAÚJO LEITE SILVA LOPES, Dr., PRESIDENTE DA CÂMARA MUNICIPAL DE BARCELOS:----------

---------- TORNA PÚBLICO o conteúdo do documento que define o quadro de políticas de segurança da informação que suportam a Estratégia Municipal de Cibesegurança do Município de Barcelos, intitulado "*POLÍTICA DE SEGURANÇA DA INFORMAÇÃO*", o qual, para o efeito, se dá em anexo por integralmente reproduzido.----------

---------- Para constar se lavrou o presente edital e outros de igual teor que vão ser publicados nos termos previstos nos n.^{os} 1 e 2 do artigo 56.º do regime jurídico das autarquias locais, aprovado em anexo à Lei n.º 75/2013, de 12 de setembro.----------

---------- Paços do Concelho de Barcelos, 10 de janeiro de 2025.----------

O PRESIDENTE DA CÂMARA MUNICIPAL,

Mário Constantino Lopes

(Mário Constantino Lopes, Dr.)

BARCELOS
MUNICÍPIO

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

A política geral de cibersegurança

Estratégia Municipal de Cibersegurança

2024

1 Propriedades do documento

Nome do ficheiro:	CIBER-POL-100-02 - Política de segurança da informação		
Versão	05	**Data da versão:**	07/11/2024
Destinatário do documento:	Todos os trabalhadores e utilizadores de entidades terceiras que estejam envolvidos em atividades de processamento de informações do Município.		
Nome do documento:	Política de segurança da informação.		
Assunto:	Documento que define a política geral de cibersegurança do Município de Barcelos.		

Aprovação e classificação da informação

1. Responsável de Cibersegurança do Município			
Elaborado por:	Henrique Necho.	**Data:**	12/03/2024
2. DSIMA			
Revisto por:	Pedro Pereira, George Araújo e José Martins.	**Data:**	24/09/2024
3. Comité de Cibersegurança			
Apreciação:	Aprovado por unanimidade.	**Data:**	07/11/2024

4. Presidência				
Aprovado por:			**Data:**	
Nível de Confidencialidade:	**X**	Informação pública.		
		Informação interna.		
		Informação confidencial.		
		Informação sigilosa.		

Controlo de versões

Versão	Data	Alterações ao documento
00	11/04/2023	Documento inicial.
01	12/03/2024	Atualizado com as informações iniciais do município.
02	19/03/2024	Atualizado com elementos de suporte ao Plano de Cibersegurança (art.° 7.° do Decreto-Lei n.° 65/2021, de 30 de julho).
03	12/04/2024	Alinhado com as categorias de controlos da ISO/IEC 27001:2022.
04	24/09/2024	Revisão do documento pela DSIMA.
05	07/11/2024	Revisão do documento pelo Comité de Cibersegurança.

2 Conteúdo do documento

3 Introdução

3.1 Preâmbulo

A segurança da informação protege a informação que nos é confiada. Um erro na segurança da informação pode ter impactos adversos significativos nos nossos trabalhadores, nos nossos munícipes, na nossa reputação e nas nossas finanças. Ao dispormos de uma **Estratégia Municipal de Cibersegurança**[1] eficaz podemos:

- Fornecer garantias do cumprimento das nossas obrigações legais, regulamentares e contratuais.
- Assegurar que as pessoas certas têm acesso certo, a dados certos, fiáveis e autênticos, no momento certo.
- Proporcionar a proteção dos dados pessoais, tal como definido no RGPD.
- Ser bons cidadãos e guardiões dos dados.

3.2 Autoridade[2]

"Enquanto organização, o tratamento da informação é fundamental para o nosso sucesso e a proteção e segurança dessa informação é uma prioridade ao nível do Município. Quer se trate de informações dos trabalhadores ou dos munícipes, levamos a sério as nossas obrigações no âmbito do Regime Jurídico da Segurança do Ciberespaço, do RGPD e restante legislação aplicável. Disponibilizámos os recursos necessários para desenvolver, implementar e melhorar de forma continua uma **Estratégia Municipal de Cibersegurança** adequada à nossa atividade, e da qual esta política é parte integrante." [Mário Constantino Araújo Leite da Silva Lopes, Dr. – Barcelos, 27 de dezembro de 2024].

Assinatura:

MARIO CONSTANTINO ARAUJO LEITE DA SILVA LOPES

Assinado de forma digital por MARIO CONSTANTINO ARAUJO LEITE DA SILVA LOPES
Dados: 2025.01.09 16:28:06 Z

1 Para conformidade com o Regime Jurídico da Segurança do Ciberespaço (Lei n.º 46/2018~, de 13 de agosto) e legislação aplicável.
2 Esta seção deve definir claramente a autoridade por trás da política. Assim, esta seção serve para estabelecer a legitimidade e a obrigatoriedade das orientações estabelecidas nesta política, demonstrando que esta não é apenas uma recomendação, mas uma exigência baseada em autoridades reconhecidas (exemplo, órgãos de direção da entidade, legislação e/ou regulamentos). Ao definir claramente a autoridade por trás da política, a organização reforça a importância da segurança da informação e fornece um fundamento sólido para a implementação e execução das práticas de segurança estabelecidas na política. Pode ser, por exemplo, uma declaração de comprometimento do órgão de direção para com a segurança da informação, realçando o seu papel no apoio e na disponibilização de recursos para a *"Estratégia Municipal da Cibersegurança"*.

4 Política de Segurança da Informação

4.1 Objetivo

O objetivo desta política é definir o quadro de políticas de segurança da informação que suportam a **Estratégia Municipal de Cibersegurança**[3] do Município de Barcelos, de forma a proteger a confidencialidade, integridade, disponibilidade e a autenticidade dos dados[4].

4.2 Âmbito de aplicação[5]

Todos os trabalhadores e utilizadores de entidades terceiras que estejam envolvidos em atividades de processamento de informações do Município.

Todos os ativos digitais considerados essenciais, detidos ou geridos pelo Município, que suportam, direta ou indiretamente, um ou mais serviços[6].

4.3 Princípio

A segurança da informação é gerida com base no risco, nos requisitos legais e regulamentares e nas necessidades do Município.

4.4 Objetivos de cibersegurança

- Assegurar a confidencialidade, a integridade, a disponibilidade e a autenticidade dos dados detidos, processados, armazenados ou transmitidos, incluindo dos dados pessoais tal como definido no RGPD, com base numa boa gestão dos riscos, nas obrigações legais, regulamentares e contratuais e nas necessidades do Município.
- Assegurar os recursos necessários para desenvolver, aplicar e melhorar continuamente a **Estratégia Municipal de Cibersegurança** do Município.
- Implementar uma cultura que potencie a adoção das melhores práticas de gestão dos riscos de cibersegurança.

[3] Para conformidade com o art.º 5.º do Regulamento n.º 183/2022 do CNCS.
[4] Considerando 79 da Diretiva SRI 2.
[5] Esta seção descreve a abrangência da política, especificando a quem é que se aplica (por exemplo, todos os funcionários e utilizadores de entidades externas) e quais os ativos que são afetados.
[6] N.º 1 do art.º 4.º do Regulamento n.º 183/2022 do CNCS.

4.5 Definição de segurança da informação

A segurança da informação é definida como a preservação de:

Confidencialidade	O acesso à informação é reservado às pessoas com autoridade adequada ***As pessoas certas com o acesso certo***
Integridade	As informações são completas e exatas ***aos dados certos***
Disponibilidade	A informação está disponível quando é necessária ***no momento certo***
Autenticidade	As informações são autênticas ***a dados fiáveis***

4.6 Quadro de políticas de segurança da informação

A **Estratégia Municipal de Cibersegurança** suporta-se, designadamente, na **estrutura da política de segurança da informação**, compostas por políticas e procedimentos agrupados em quatro categorias[7] - políticas organizacionais, políticas de utilizador, políticas de controlo físico e políticas tecnológicas.

Em conjunto com esta política, as seguintes políticas de segurança da informação constituem o quadro de políticas:

4.6.1 Políticas ao Nível Organizacional[8]

- CIBER-POL-100-01 - Estratégia Municipal de Cibersegurança*

[7] Esta disposição ajuda a garantir uma abordagem estruturada e abrangente da segurança da informação dentro da organização. Cada nível tem um foco específico e aborda diferentes aspetos da segurança da informação, contribuindo para uma estrutura sólida e integrada. As categorias de políticas estão alinhadas com as categorias de controlo definidas na norma ISO/IEC 27001:2022
8 As políticas ao nível organizacional definem a abordagem global da organização em relação à segurança da informação. Estas estabelecem os princípios orientadores, os objetivos estratégicos e o compromisso dos órgãos de direção para com a segurança da informação. Estas são políticas de alto nível e fornecem a estrutura dentro da qual todas as outras políticas e procedimentos de segurança são desenvolvidos

- CIBER-POL-100-02 - Política de Segurança da Informação* (esta política)
- CIBER-POL-100-03 - Estrutura da política de segurança da informação*
- CIBER-POL-100-04 - Registo de requisitos legais, contratuais e outros*
- CIBER-POL-100-05 - Política e procedimentos de gestão do risco*
- CIBER-POL-100-06 - Política de Gestão e Notificação de Incidentes de Cibersegurança *
- CIBER-POL-100-07 - Política de classificação e tratamento da informação
- CIBER-POL-100-08 - Requisitos de cibersegurança nos procedimentos de contratação

4.6.2 Políticas ao Nível do Utilizador[9]

- CIBER-POL-200-01 - Funções e responsabilidades na segurança da informação*
- CIBER-POL-200-02 - Política e plano de formação e sensibilização em matéria de cibersegurança*
- CIBER-POL-200-03 - Política de gestão da palavra-passe
- CIBER-POL-200-04 - Política de autenticação multifator

4.6.3 Políticas de Controlo Físico

- CIBER-POL-300-01 – Política de Acesso e Controlo Físico

4.6.4 Políticas ao Nível Tecnológico[10]

- CIBER-POL-400-01 - Política de gestão de ativos*
- CIBER-POL-400-02 - Política de gestão de cópias de segurança

4.6.5 Outros documentos de conformidade regulatória

- CIBER-POL-500-01 - Inventariação dos ativos*
- CIBER-POL-500-02 - Lista de ativos*
- CIBER-POL-500-03 - Diagrama de arquitetura de comunicação de dados*
- CIBER-POL-500-04 - Registo dos riscos (*risk register*)*

9 As políticas ao nível do utilizador são direcionadas aos utilizadores individuais dentro da organização, incluindo funcionários, contratados e terceiros, fornecendo orientações sobre as expectativas de comportamento seguro e uso responsável dos recursos de TI. Estas políticas ajudam a garantir que todos os utilizadores estejam cientes das suas responsabilidades em relação à segurança da informação.
10 As políticas ao nível de sistema e de controlo especificam os requisitos para a segurança dos sistemas de informação e os controlos que devem ser implementados para proteger as informações. Estas políticas são técnicas e detalhadas, abordando a segurança ao nível dos sistemas, das aplicações e da rede.

- CIBER-POL-500-05 - Plano de Tratamento dos Riscos*
- CIBER-POL-500-06 - Relatório Anual sobre Cibersegurança*
- CIBER-POL-500-07 - Acordo de confidencialidade

** Políticas e Relatórios obrigatórias no âmbito do RJSC*

4.7 Funções e Responsabilidades[11]

A segurança da informação é da responsabilidade de todos, que devem compreender e cumprir as políticas, seguir os processos e procedimentos definidos, designadamente, comunicar incidentes suspeitos ou em curso. As funções e responsabilidades específicas para o funcionamento do pograma de segurança da informação são definidas e registadas no documento **funções e responsabilidades na segurança da informação**.

4.8 Monitorização

A conformidade com as políticas e os procedimentos da **Estratégia Municipal de Cibersegurança** é monitorizada periodicamente pelo Responsável de Cibersegurança, com o apoio da DSIMA e, se necessário, por análises independentes efetuadas pela Auditoria Interna e Externa.

4.9 Obrigações legais e regulamentares

O Município de Barcelos cumpre com as suas obrigações legais, regulamentares e contratuais, e estes requisitos estão documentados no **registo de requisitos legais e contratuais**. Este registo justifica o quadro de políticas e procedimentos de segurança da informação adotado [4.6].

4.10 Formação e sensibilização

As políticas e os procedimentos estão disponíveis para todos os trabalhadores e utilizadores de entidades terceiras, na intranet do município, se necessário.

11 Esta secção enumera as várias funções envolvidas na política e na sua aplicação, bem como as suas responsabilidades na implementação, adesão ou cumprimento das disposições estabelecidas na política. As funções típicas incluem os Órgãos de Direção, Responsável da Cibersegurança (CISO), Diretor das Tis ou utilizadores finais

Está em vigor um plano de formação e sensibilização relativamente às políticas, processos e conceitos de cibersegurança. As necessidades e os requisitos de formação estão registados no **plano de formação em cibersegurança**.

4.11 Melhoria contínua do plano municipal

A **Estratégia Municipal de Cibersegurança** é continuamente melhorada. A política de melhoria contínua define a abordagem da organização em relação a esta problemática, existindo para esse efeito um processo em vigor.

5 Conformidade da política

5.1 Medição da conformidade

O Responsável de Cibersegurança, com o apoio da DSIMA, verificará a conformidade com esta política através de vários métodos, incluindo, mas não se limitando a, relatórios de ferramentas de trabalho, auditorias internas e externas e informação de feedback do proprietário da política.

5.2 Exceções

Qualquer exceção a esta política deve ser previamente aprovada e documentada pelo Responsável de Cibersegurança e comunicada ao responsável da DSIMA.

5.3 Não conformidade

Um trabalhador que tenha violado esta política pode ser objeto de um procedimento disciplinar.

5.4 Revisão e avaliação

Esta política é atualizada e revista como parte do processo de melhoria contínua, com uma periodicidade anual ou sempre que se justifique.

6 Definições principais[12]

6.1 Terminologia

Termo	Definição	Origem
Ativo	Qualquer coisa que tenha valor para uma organização	ISO/IEC 22000
Ativos digitais	Os ativos digitais são todos os sistemas de informação e comunicação, os equipamentos e os demais recursos físicos e lógicos considerados essenciais, geridos ou detidos pela entidade, que suportam, direta ou indiretamente, um ou mais serviços	Regulamento nº 183/2022 do CNCS
Cibersegurança	Conjunto de medidas e ações de prevenção, monitorização, deteção, reação, análise e correção que visam manter o estado de segurança desejado e garantir a confidencialidade, integridade, disponibilidade e não repúdio da informação, das redes e sistemas de informação no ciberespaço, e das pessoas que nele interagem	ENSC
Framework	Modelo de referência	NP ISO/IEC 27001
Órgãos de direção	Pessoa ou grupo de pessoas que dirige e controla uma organização ao mais alto nível	Diretiva SRI 2
Melhoria contínua	Atividade recorrente com vista a incrementar a capacidade para satisfazer requisitos	NP EN ISO 9000
Política	Intenções e orientação de uma organização, conforme formalmente expressas pela sua gestão de topo	NP EN ISO 22301
Rede e sistema de informação	Qualquer dispositivo ou conjunto de dispositivos interligados ou associados, em que um ou mais desenvolve, em execução de um programa, o tratamento automatizado de dados informáticos, bem como a rede de comunicações eletrónicas que suporta a comunicação	Lei 46/2018

12 Nesta seção são fornecidas definições claras de termos técnicos, termos e abreviaturas utilizados na política para garantir que todos os destinatários, independentemente de seu nível de conhecimento técnico, possam compreender o conteúdo e assim evitar mal-entendidos.

	entre eles e o conjunto de dados informáticos armazenados, tratados, recuperados ou transmitidos por aquele ou aqueles dispositivos, tendo em vista o seu funcionamento, utilização, proteção e manutenção	
Responsável de Cibersegurança	Pessoa designada como responsável de segurança para a gestão do conjunto das medidas adotadas em matéria de requisitos de segurança e de notificação de incidentes, nos termos do Regime Jurídico da Segurança do Ciberespaço e legislação aplicável (n.º 1 do art.º 5 do Decreto-Lei n.º 65/2021, de 30 de julho)	
Segurança das redes e dos sistemas de informação	A capacidade das redes e dos sistemas de informação para resistir, com um dado nível de confiança, a ações que comprometam a confidencialidade, integridade, disponibilidade, autenticidade e o não repúdio dos dados armazenados, transmitidos ou tratados, ou dos serviços conexos oferecidos por essas redes ou por esses sistemas de informação, ou acessíveis através dos mesmos	Lei 46/2018
Serviço essencial	Um serviço essencial para a manutenção de atividades societais ou económicas cruciais, que dependa de redes e sistemas de informação, e em relação ao qual a ocorrência de um incidente possa ter efeitos perturbadores relevantes na prestação desse serviço	Lei 46/2018
Sistema de gestão	Conjunto de elementos inter-relacionados ou interatuantes de uma organização para o estabelecimento de políticas, objetivos e de processos para atingir esses objetivos	NP EN ISO 22301

6.1 Abreviaturas

Abreviatura	Definição
CISO	Chief Information Security Officer – Responsável de Segurança de Informação
CNCS	Centro Nacional de Cibersegurança
GNS	Gabinete Nacional de Segurança
ENSC	Estratégia Nacional de Cibersegurança

ISO/IEC	International Organization for Standardization/International Electrotechnical Commission
QNRSC	Quadro Nacional de Referência para a Cibersegurança
QACC	Quadro de Avaliação de Capacidades de Cibersegurança
RGPD	Regulamento Geral sobre a Proteção de Dados
RJSC	Regime Jurídico da Segurança do Ciberespaço, Lei n.º 46/2018, de 13 de agosto, regulamentado pelo Decreto-Lei n.º 65/2021, de 30 de julho

7 Referências

Para a realização desta política, são tidas como referências as seguintes fontes:

- Lei 46/2018, de 13 de agosto (RJSC)
- Decreto-Lei n.º 65/2021, de 30 de julho (Regulamentação do RJSC)
- Instrução Técnica - Regulamento n.º 183/2022 do CNCS
- Aviso n.º 1517/2024, de 22 de janeiro, do Gabinete Nacional de Segurança
- Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho de 6 de julho de 2016, relativa à segurança das redes e da informação em toda a União (Network and Information Security Directive - NIS)
- Diretiva (UE) 2022/2555 que estabelece medidas destinadas a garantir um elevado nível comum de cibersegurança na União, com vista a melhorar o funcionamento do mercado interno (Diretiva SRI 2)
- Diretiva (UE) 2022/2555 do Parlamento Europeu e do Conselho de 14 de dezembro de 2022 (Diretiva SRI 2 ou NIS 2 Directive) – atualmente em processo de transposição – relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança na União
- Quadro Nacional de Referência para a Cibersegurança (CNCS, 2019)
- Quadro de Avaliação de Capacidades de Cibersegurança (CNCS, 2020)
- Guia para Gestão dos Riscos em matérias de Segurança da Informação e Cibersegurança (CNCS, 2023)
- European Cybersecurity Skills Framework (ENISA, 2022)
- ISO/IEC 27001:2022 - Information security, cybersecurity and privacy protection - Information security management systems requirements

- ISO/IEC 27002:2022 - Information security, cybersecurity and privacy protection - Information security controls
- ISO/IEC 27005:2022 - Information security, cybersecurity and privacy protection - Guidance on managing information security risks
- NIST SP 800-30 Rev. 1, Guide for Conducting Risk Assessments
- NIST SP 800-37 Rev. 2, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy.
- Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (RGPD)
- Lei n.º 58/2019, de 08 de agosto, Lei da Proteção de Dados Pessoais
- Constituição da República Portuguesa - CRP - Artigo 35.º