Despacho

Assunto: Nomeações internas do Responsável de Cibersegurança e Ponto de Contacto Permanente perante o executivo, ao abrigo do Decreto-Lei n.º 125/2025 de 4 de dezembro, relativo ao Regime Jurídico da Cibersegurança.

Considerando que:

1º - A 3 de abril de 2026, entrou em vigor o Decreto-Lei n.º 125/2025, de 04 de dezembro, que aprova o Regime Jurídico da Cibersegurança, transpondo a Diretiva (UE) 2022/2555, do Parlamento Europeu e do Conselho, de 14 de dezembro de 2022, destinada a garantir um elevado nível comum de cibersegurança em toda a União;

2º - As disposições deste novo quadro normativo, articuladas com o Quadro Nacional de Referência para a Cibersegurança (QNCS), definem exigências rigorosas em matéria de gestão de risco tecnológico, proteção da informação e defesa das infraestruturas da Administração Pública Local;

3º - Este novo regime jurídico obriga à designação formal de responsáveis para a gestão do conjunto das medidas adotadas em matéria de requisitos de cibersegurança e de notificação de incidentes às autoridades competentes;

4º - A alínea a), do n.º 3, do artigo 3º e a alínea d), do n.º 1, do artigo 6º deste Decreto-Lei n.º 125/2025, de 04 de dezembro classificam as autarquias locais como entidades essenciais do sector «*Administração Pública*»;

5º - O n.º 1, do artigo 31º deste novo Regime Jurídico dispõe que as entidades essenciais designam um responsável de cibersegurança para a gestão da cibersegurança e da segurança da informação, que seja titular dos órgãos de gestão, direção ou administração ou lhes responda organicamente e de forma direta;

6º - Por sua vez, o artigo 32º deste diploma legal estipula que as entidades essenciais e importantes designam um ponto de contacto permanente, que pode ser assegurado por um elemento;

Designo, Paulo Alexandre Cardoso Gonçalves, Técnico de Sistemas e Tecnologias de Informação, como Responsável da Cibersegurança desta autarquia, nos termos do disposto no supra citado

Largo Hermenegildo Solheiro
4960-551 Melgaço

Telf. 251 410 100

www.cm-melgaco.pt
geral@cm-melgaco.pt

artigo 31º, n.º 1 do Decreto-Lei n.º 125/2025, de 04 de dezembro, devendo qualquer contacto relativo a esta temática ser endereçado para o endereço de correio eletrónico responsavel.seguranca@cm-melgaco.pt, ou para o telefone n.º +351 251 410 100 / telemóvel n.º +351 927525121.

Mais determino, nos termos do disposto no artigo 32º do citado diploma legal, que o Ponto de Contacto Permanente, é o mesmo, Técnico de Sistemas e Tecnologias de Informação, Paulo Alexandre Cardoso Gonçalves, através do endereço de correio eletrónico principal contacto.permanente@cm-melgaco.pt ou pelos endereços de correio eletrónico alternativos informatica@cm-melgaco.pt e geral@cm-melgaco.pt ou, ainda, pelo telefone n.º +351 251 410 100 / telemóvel n.º +351 927525121.

Melgaço, 12 de junho de 2026

O Presidente da Câmara Municipal,

JOSÉ ALBANO ESTEVES DOMINGUES

Assinado de forma digital por JOSÉ ALBANO ESTEVES DOMINGUES
Dados: 2026.06.18 20:46:17 +01'00'

(José Albano Esteves Domingues)

Largo Hermenegildo Solheiro
4960-551 Melgaço

Telf. 251 410 100

www.cm-melgaco.pt
geral@cm-melgaco.pt

NOTA INFORMATIVA

Responsável de Cibersegurança e Ponto de Contacto Permanente

ASSUNTO: REGIME JURÍDICO DA CIBERSEGURANÇA - DECRETO-LEI N.º 125/2025

Conteúdo

Largo Hermenegildo Solheiro
4960-551 Melgaço

Telf. 251 410 100

www.cm-melgaco.pt
geral@cm-melgaco.pt

A. CONTEXTO

Na sequência da entrada em vigor do Decreto-Lei 125/2025 de 4 de dezembro, que Transpõe a Diretiva (UE) 2022/2555, relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança na União, e que aprova regime jurídico da cibersegurança, destacamos os seguintes pontos a considerar:

- O Regime Jurídico da Cibersegurança (doravante RJC), define os requisitos de segurança das redes e sistemas de informação, as regras para a notificação de incidentes, que devem ser cumpridos pelas Entidades Essenciais, entidades importantes e Administração Pública.
- As entidades referidas no ponto anterior devem:
    - Inscrever-se na plataforma eletrónica a disponibilizar pelo Centro Nacional de Cibersegurança;
    - Implementar um Sistema de gestão de riscos de cibersegurança e consequentes medidas de cibersegurança;
    - Designar um Responsável de Cibersegurança para a gestão da cibersegurança e da segurança da informação, que seja titular dos órgãos de gestão, direção ou administração ou lhes responda organicamente e de forma direta;
    - Indicar pelo menos, um ponto de contacto permanente, de modo a assegurar os fluxos de informação de nível operacional e técnico com o Centro Nacional de Cibersegurança;
    - Elaborar uma análise de risco por ativo;
    - Elaborar um relatório anual e
    - Proceder à identificação, análise e eventual notificação de incidentes de segurança.

No seguimento do projeto de implementação dos requisitos previstos no Decreto-Lei 125/2025 de 4 de dezembro, cabe fazer uma análise casuística dos recursos, competências e funções das figuras do **Responsável de Cibersegurança** e do **Ponto de Contacto Permanente**.

Considerando que o Município de Melgaço é uma entidade que opera no sector da Administração Pública em Portugal, sector especificamente previsto no Regime Jurídico de Cibersegurança, qualificando-se como Entidade essencial, nos termos do art.º 6.º e anexo I do RJC, terá de cumprir com as obrigações

Largo Hermenegildo Solheiro
4960-551 Melgaço

Telf. 251 410 100

www.cm-melgaco.pt
geral@cm-melgaco.pt

identificadas, nomeadamente a identificação de um Responsável de Cibersegurança e de um Ponto de Contacto Permanente. Nestes termos somos a apresentar, um resumo relativamente às funções indicadas.

B. RESPONSÁVEL DE CIBERSEGURANÇA

A função de **Responsável de Cibersegurança**, é uma função exercida na entidade com o objetivo de garantir a segurança de informação dessa mesma entidade, através da gestão do conjunto das medidas adotadas em matéria de requisitos de segurança e de notificação de incidentes.

Trata-se de uma posição de gestão, com responsabilidades na organização, inerentes ao desempenho desse cargo. Nesse sentido se entende que o/a Responsável de Cibersegurança não pode ser externalizado, sem prejuízo de serviços de consultoria e/ ou suporte que a entidade entenda adquirir por via externa

- O/A **Responsável de Cibersegurança** deve reportar diretamente à gestão de topo, ou pertencer à gestão de topo da entidade. Dado que o impacto da sua responsabilidade é potencialmente transversal, deve ter conhecimento pleno dos processos chave da entidade onde se insere quer do ponto de vista técnico, quer do ponto de vista de negócio / atividade, devendo ser capaz de reencaminhar internamente as solicitações das Autoridades;

O/A **Responsável de Cibersegurança** deve ser capaz de traduzir os objetivos da entidade em requisitos de segurança de informação:

- O/A **Responsável de Cibersegurança** tem as seguintes funções:
  - Propor as medidas de gestão dos riscos de cibersegurança, incluindo ao nível da cadeia de abastecimento;
  - Prestar informações relativas às medidas de gestão dos riscos de cibersegurança aos órgãos da entidade responsável pela sua supervisão;
  - Auxiliar os órgãos da entidade no cumprimento das medidas de supervisão e de execução;
  - Contribuir para a promoção de uma cultura de cibersegurança na entidade, propondo, nomeadamente, as ações de formação em cibersegurança;
  - Assegurar a gestão de riscos de cibersegurança
  - Assegurar o cumprimento das obrigações referentes à elaboração do relatório anual

Largo Hermenegildo Solheiro
4960-551 Melgaço

Telf. 251 410 100

www.cm-melgaco.pt
geral@cm-melgaco.pt

- Coordenar as ações do ponto de contacto permanente
- Acompanhar todo o processo de implementação, definição de prioridades e atividades de melhoria continua, que garantam que a entidade está preparada em termos de segurança da informação e cibersegurança;
- Assegurar a definição, implementação e manutenção da estratégia de Segurança da Informação e Ciberseguranca de forma holística e estruturada;
- Ter conhecimento e garantir implementação de boas práticas de Segurança da Informação e Ciberseguranca, como o "Quadro Nacional de Referência para a Ciberseguranca" e "ISO/IEC 27001";
- Assegurar o desenvolvimento e implementação de políticas, processos e procedimentos de Ciberseguranca;
- Definir e implementar estratégias de avaliação e de resposta aos riscos
- Acompanhar e avaliar a execução nomeadamente dos processos de Gestão de Alterações e de Gestão de Incidentes;
- Acompanhar auditorias de Ciberseguranca e garantir a implementação de ações de melhoria para mitigação do risco;
- Suportar a entidades na estratégia, desempenho e monitorização dos sistemas aplicacionais e infraestrutura;
- **Assinar** e **elaborar**:
    - Inventário de Ativos;
    - Lista de Ativos;
    - Relatórios Anuais.

- A designação do/a **Responsável de Cibersegurança** deve ser comunicada ao Centro Nacional de Ciberseguranca no <u>prazo de 20 dias úteis a contar da data de entrada em vigor do RJC (4 de maio de 2026);</u>
- A informação a constar da comunicação a enviar ao Centro Nacional de Ciberseguranca deve conter o detalhe documentado em regulamento a aprovar por esta entidade, devendo conter pelo menos:
    - Nome da entidade;

Largo Hermenegildo Solheiro
4960-551 Melgaço
Telf. 251 410 100
www.cm-melgaco.pt
geral@cm-melgaco.pt

- Nome do/a Responsável de cibersegurança;
- Cargo do/a Responsável de cibersegurança;
- Endereço de correio eletrónico;
- Número de telefone fixo; e
- Número de telefone móvel.

C. PONTO DE CONTACTO PERMANENTE

Tendo em conta a importância e o impacto da Segurança da Informação nas entidades e as necessidades que têm surgido ao longo do tempo bem como as ameaças e incidentes que associadas, torna-se fundamental que as entidades assegurem a função de Ponto de contacto disponível de modo a assegurar os fluxos de informação de nível operacional e técnico com o Centro Nacional de Cibersegurança, nomeadamente:

- A função do Ponto de Contacto Permanente torna-se fundamental para assegurar:
    - Os fluxos de informação de nível operacional e técnico com a autoridade de cibersegurança competente, nomeadamente:
        - A articulação intersectorial, incluindo a eficácia da resposta a incidentes de segurança com impacto a nível dos setores;
        - A obtenção de informação operacional e técnica, na sequência de notificação de incidentes com impacto significativo submetida pela mesma ou por outra entidade;
        - A obtenção e atualização de informação de situação integrada no contexto de um incidente significativo;
    - A partilha de informação com a autoridade de cibersegurança competente, quando estejam ativados planos de emergência de proteção civil diretamente relacionados ou com impacto ao nível da cibersegurança bem como de planos no âmbito do planeamento civil de emergência da cibersegurança, dos planos de segurança das infraestruturas críticas nacionais ou europeias, ou dos planos de resiliência das entidades críticas nacionais ou europeias;

Largo Hermenegildo Solheiro
4960-551 Melgaço
Telf. 251 410 100
www.cm-melgaco.pt
geral@cm-melgaco.pt

- A operacionalização dos procedimentos fixados no âmbito de um plano de emergência de proteção civil quando tenham impacto no funcionamento das redes e sistemas de informação, ou do planeamento civil de emergência da cibersegurança;
- A receção das orientações, recomendações, instruções técnicas e ordens emitidas pela autoridade de cibersegurança competente.

- O Ponto de contacto permanente deve manter disponibilidade contínua de 24 horas por dia e de sete dias por semana, limitada a períodos de ativação, iniciados e terminados mediante comunicação do Centro Nacional de Cibersegurança.
- O Ponto de Contacto Permanente poderá ser:
  - uma pessoa;
  - um departamento interno;
  - um departamento externo através de contratação de serviço;
- A escolha do Ponto de Contacto Permanente deverá ser realizada pela entidade e o mesmo deverá:
  - conhecer os procedimentos e ações a tomar nos vários cenários previstos e categorizados que possam surgir;
  - utilizar os canais apropriados e definidos para este tipo de circunstâncias;
  - ter disponibilidade total de resposta nos períodos de ativação, de forma a garantir o suporte devido à entidade, mitigando riscos para a operação e para o negócio;
- Caso seja indicado o contacto geral da entidade como Ponto de Contacto Permanente recomenda-se a existência de procedimentos adequados para reencaminhamento dos contactos para uma resposta adequada;
- A designação do Ponto de contacto permanente deveria ser comunicada ao Centro Nacional de Ciberseguranca no prazo de 20 dias úteis a contar da data de entrada em vigor do RJC (4 de maio de 2026);
- A informação a enviar ao Centro Nacional de Ciberseguranca deve conter o detalhe documentado em regulamento a aprovar por esta entidade, devendo conter pelo menos:
  - Nome da entidade;
  - Nome do ponto ou pontos de contacto permanente / serviço disponível ou equipa operacional;

Largo Hermenegildo Solheiro
4960-551 Melgaço

Telf. 251 410 100

www.cm-melgaco.pt
geral@cm-melgaco.pt

- Endereço de correio eletrónico principal;
- Endereço de correio eletrónico alternativo;
- Número de telefone fixo principal, se aplicável;
- Número de telefone móvel principal;
- Número de telefone fixo alternativo, se aplicável;
- Número de telefone móvel alternativo;
- Outros contactos alternativos.

Município de Melgaço

Sistema de Gestão da qualidade e Modernização Administrativa

Largo Hermenegildo Solheiro
4960-325 Melgaço
Telf. 251 410 100
www.cm-melgaco.pt
geral@cm-melgaco.pt