**Anexo II**

**Matriz de Risco de Segurança e Cibersegurança**

**Vouchers para Startups – TD- C16-i02**

(Modelo proposto)

|  |  |  |
| --- | --- | --- |
| **Riscos associados** | **Especificação do risco** | **Medidas de mitigação** |
| R1 | • Omissão de riscos específicos ao nível dos projetos ou componentes dos mesmos. | • M1, M3 |
| R3 | • Má conceção e configuração de plataformas, software, redes e sistemas que causem quebras na cibersegurança dos mesmos e coloquem em risco, por exemplo, os dados alojados. | • M1, M3, M6, M7 e M13 |
| R4 | •Interferência de terceiros em plataformas, software, redes e sistemas que coloquem em risco, por exemplo, os dados alojados. | • M1, M2, M3, M4, M5, M6, M7, M8, M9 e M13 |
| R5 | • Participação de empresas subcontratadas na conceção e gestão. | • M5 e M6 |
| R6 | • Não cumprimento das disposições do RGPD. | • M5, M7 e M13 |
| R8 | • Dependência de fornecedores e tecnologias especificas (“*vendor-locking*”). | • M10 |
| R9 | • Falta de confiança de consumidores na utilização de plataformas e sistemas. | • M11 e M13 |
| R10 | • Requisitos técnicos de cibersegurança insuficientes ou incorretos. | •M1, M3, M4, M5, M6, M7, M9 e M13 |
| R12 | • Utilização de plataformas, software, redes e sistemas que não tenham as atualizações de segurança mais recentes, fornecidas pelos fabricantes. | • M2, M3, M7, M9, M10 e M12 |

Nota: A matriz proposta identifica os principais riscos e as principais medidas de mitigação, sendo considerados apenas riscos que, no caso concreto, tenham impacto médio-elevado e/ou probabilidade média-elevada (sem prejuízo da identificação de outros).

**Medidas de Mitigação**

M1 – Desenvolvimento de plano de risco detalhado, com medidas de mitigação especificas no âmbito da efetiva concretização da medida, submedida ou projeto.

M2 – Formação de cibersegurança, de acordo com as melhores práticas e recomendações e de acordo com o nível de responsabilidade do utilizador ou responsável.

M3 – Especificações de cibersegurança desenvolvidas e/ou auditadas com especialistas.

M4 – Articulação operacional e técnica com o Centro Nacional de Cibersegurança.

M5 – Identificação do Encarregado de Proteção de Dados (EPD) da plataforma e/ou do EPD ao nível da organização implementadora/beneficiário final.

M6 – Exigência de credenciação de segurança por parte do fornecedor, adequada ao risco da plataforma e ou do sistema.

M7 – Desenvolvimento de ações de auditoria de cumprimento do Regulamento Geral sobre a Proteção de Dados (RGPD) e de cibersegurança a sistemas e plataformas.

M8 – Aplicação de restrições a fornecedores considerados de alto-risco.

M9 – Implementar sistemas de backup e/ou redundância de sistemas críticos.

M10 – Especificações técnicas que permitam a apresentação de propostas alternativas em sede de concurso e que impliquem, sempre que possível, a interoperabilidade entre sistemas.

M11 – Aprovação de iniciativas de certificação em matéria de cibersegurança.

M12 - Promoção de mecanismos de atualização automática, nomeadamente através da utilização de soluções “*cloud by default*”.

M13 – Utilização de sistemas com fator de dupla autenticação e/ou identidade digital, como o caso da Chave Móvel Digital ou futuramente a eID.