Autoridade Nacional da Aviação Civil
Portuguese Civil Aviation Authority

Política de Segurança da Informação (POSI)

A POSI visa estabelecer princípios, diretrizes e responsabilidades que devem ser cumpridos por todos os intervenientes que, no âmbito da sua atividade, tenham acesso a informação da ANAC (**colaboradores, parceiros, regulados e terceiros**), aplicando-se também a todos os **sistemas de informação, ativos tecnológicos, infraestruturas críticas e documentos físicos** sob gestão da ANAC. A salvaguarda da informação sob gestão da ANAC deve respeitar integralmente a **legislação nacional, europeia e internacional e também a aplicável ao domínio da aviação civil.**

Princípios Fundamentais

1. **Confidencialidade**: Garantir que a informação é acessível apenas a pessoas autorizadas.
2. **Integridade**: Assegurar que os dados são exatos, completos e protegidos contra alterações não autorizadas.
3. **Disponibilidade:** Garantir que a informação e os sistemas estão disponíveis sempre que necessário.
4. **Autenticidade**: Confirmar a identidade das partes envolvidas no acesso e tratamento da informação.
5. **Rastreabilidade:** Registar e monitorizar acessos e ações relevantes sobre os sistemas e dados da ANAC.
6. **Legalidade**: Cumprimento do Regulamento Geral de Proteção de Dados (RGPD), legislação nacional de cibersegurança e normas internacionais da aviação civil.
7. **Proporcionalidade**: Implementar medidas de segurança adequadas ao nível de risco identificado.

Diretrizes Gerais

1. **Gestão de Riscos**: A ANAC deve manter um processo contínuo de identificação, avaliação e mitigação de riscos de segurança da informação, tendo também em conta o seu impacto na segurança operacional.
2. **Classificação da Informação**: Os dados, sempre que seja considerado necessário, devem ser classificados (público, restrito, confidencial, reservado) e protegidos de acordo com o seu nível de sensibilidade.

3. **Controlo de Acessos**: O acesso à informação deve ser baseado no princípio da necessidade de conhecer e revisto periodicamente, privilegiando o trabalho colaborativo (o conhecimento deve ser disseminado entre os membros da equipa, evitando a sua individualização).
4. **Proteção de Dados Pessoais**: O tratamento de dados pessoais deve respeitar o RGPD, garantindo transparência, minimização e limitação da finalidade.
5. **Segurança Física e Lógica**: Instalações e sistemas da ANAC devem ser protegidos contra intrusão, falhas e desastres.
6. **Continuidade de Negócio**: Devem existir planos de continuidade e recuperação de desastres testados periodicamente.
7. **Gestão de Incidentes**: Todos os incidentes de segurança devem ser registados, analisados e comunicados, com mecanismos de resposta rápida.
8. **Sensibilização e Formação**: Todos os colaboradores devem receber formação periódica sobre segurança da informação e proteção de dados.
9. **Fornecedores e Terceiros**: Contratos com prestadores de serviços devem incluir cláusulas de segurança da informação e confidencialidade.
10. **Monitorização e Gestão da Qualidade:** Devem ser implementados processos de monitorização e controlo da qualidade, que assegurem o alinhamento da segurança da informação com os objetivos estratégicos da ANAC, que permitam avaliar a eficácia dos controlos e garantir a melhoria contínua.

A Presidente do Conselho de Administração