ANAC
Autoridade Nacional da Aviação Civil
Portuguese Civil Aviation Authority

Política de Cibersegurança

A transformação digital aumentou, por um lado, a dependência das organizações a tecnologias digitais e, por outro, a exposição das mesmas a **ameaças cibernéticas**, sobressaindo, neste contexto, o papel da cibersegurança enquanto área multidisciplinar que protege a segurança de dados, sistemas, redes, pessoas e outras áreas críticas. Ciente desta realidade em permanente evolução, a Autoridade Nacional da Aviação Civil (ANAC) adota a presente **Política de Cibersegurança**, com o objetivo central de criar um ambiente seguro para as atividades que desenvolve em ambiente digital, garantindo a **confidencialidade, integridade e disponibilidade** dos seus sistemas de informação, e que se consubstancia nas seguintes diretrizes:

Identificação: é realizado e mantido atual o mapeamento de ativos digitais e é promovida a avaliação contínua dos riscos associados a esses ativos, com identificação e priorização das vulnerabilidades e ameaças, bem como a implementação de medidas adequadas para as mitigar.

Proteção: são instituídas regras de gestão de acessos com base no princípio do "menor privilégio" e autenticação multifator para o acesso a sistemas críticos; são implementados sistemas de proteção de redes e sistemas, como firewalls, VPN e encriptação de dados, e de proteção contra malware, como antivírus e antimalware; é assegurada a proteção de dados, garantindo a conformidade com o RGPD, o backup regular e a eliminação segura de dados; e é realizado o controle rigoroso sobre dispositivos que acedem à rede.

Deteção e monitorização: são realizadas auditorias regulares, para verificar a conformidade e a vulnerabilidade dos equipamentos, redes e software; é assegurada a monitorização contínua dos sistemas, para deteção de intrusões e atividades suspeitas; e são mantidos e analisados registos de atividades (logs), para assegurar a integridade, a rastreabilidade e conformidade da utilização.

Resposta e Recuperação: são estabelecidas regras de reporte de ocorrências de cibersegurança, são delineados e seguidos procedimentos de resposta a incidentes cibernéticos, incluindo investigação, contenção da ameaça, recuperação dos sistemas, notificação e mitigação de violações de dados; é promovida a cooperação Interinstitucional, incluindo a partilha de informações sobre ciberameaças e a coordenação de esforços de combate.

Cultura e formação: é fomentado o desenvolvimento de uma cultura organizacional atenta e empenhada na segurança digital, focada na prevenção e gestão de risco e consciente da responsabilidade partilhada, através da capacitação, sensibilização e formação continuada dos utilizadores para as ameaças cibernéticas e para as regras e boas práticas de mitigação dos riscos e de proteção de dados.

A Presidente do Conselho de Administração

Ana Vieira da Mata