O objetivo da Política de Segurança da Informação da CASO é a definição das diretivas para a organização e para a proteção dos seus ativos de informação contra todas as ameaças internas, externas, deliberadas ou acidentais.

Assim, no âmbito do SGSTI da CASO foram estabelecidos os seguintes princípios de atuação no que concerne à Segurança da Informação:

- O objetivo da Gestão da Segurança da Informação na CASO é garantir a proteção dos seus ativos de informação, a continuidade do seu negócio e a mitigação dos seus riscos, prevenindo os incidentes de segurança e reduzindo o seu potencial impacto.
- A Política de Segurança garante que:
  - . os ativos de informação estão protegidos contra todos os acessos não autorizados;
  - . a confidencialidade da informação está preservada;
  - . a integridade e disponibilidade da informação são mantidas;
  - . os requisitos legais, legislativos, regulatórios e contratuais são cumpridos;
  - . o Plano de Continuidade do negócio é definido, mantido e testado;
  - . todos os incidentes relacionados com a segurança da informação são reportados e adequadamente investigados;
  - . todas as equipas estão comprometidas e colaboram ativamente para o cumprimento da Política de Segurança e a melhoria contínua do SGSTI da CASO.
- A Política de Segurança é suportada por outras políticas e restante documentação do SGSTI.
- O responsável do processo de Segurança da Informação é responsável pela manutenção da Política de Segurança e pelo suporte e aconselhamento durante a sua implementação.
- Devem manter-se controlos adequados de segurança, com revisões e atualizações periódicas, pelo menos uma vez por ano; a eficácia dos controlos implementados é avaliada através de auditorias internas de segurança específicas;
- Para os serviços de TI que impliquem o acesso de organizações externas aos sistemas da CASO, são aplicáveis as cláusulas de segurança estabelecidas nos contratos respetivos;
- Todos os processos do SGSTI devem considerar os níveis de Segurança da Informação da CASO;
- Todos os responsáveis de processo são responsáveis pela implementação e cumprimento da Política de Segurança da Informação nas suas respetivas áreas.
- O cumprimento da Política de Segurança da Informação é obrigatório.
- Devem analisar-se os riscos sobre a infraestrutura, serviços e organização de TI da CASO, segundo a perspetiva da Segurança da Informação, e de acordo com os critérios de confidencialidade, integridade e disponibilidade.
- As alterações com implicações na Segurança da Informação deverão ser validadas pelo processo de Gestão de Segurança da Informação conjuntamente com o processo de Gestão de Alterações;
- As modificações que se realizem sobre documentos e/ou anexos com conteúdo de Segurança da Informação, deverão ser validadas pelo processo de Gestão de Segurança da Informação.