

# CIBERSEGURANÇA NA ADMINISTRAÇÃO PÚBLICA

O IMPERATIVO DA CONFORMIDADE GLOBAL NO SNS



# ENCONTROS SAMA<sup>2020</sup>

26 ABRIL 14h30-17h15  
LISBOA

**ama** AGÊNCIA PARA A  
MODERNIZAÇÃO  
ADMINISTRATIVA

**COMPETE  
2020**

**PORTUGAL  
2020**



# ÍNDICE

- SÍNTESE DO PROJETO
- A CONFORMIDADE GLOBAL NO SNS
- IMPLEMENTAÇÃO DE UMA METODOLOGIA TRANSVERSAL E ESTRUTURADA – FUNDAMENTOS
- DEFINIÇÃO DOS OBJETIVOS ESTRATÉGICOS E EIXOS DE INTERVENÇÃO
- CRONOGRAMA TEMPORAL DOS EIXOS DE INTERVENÇÃO & LINHAS DE AÇÃO



## SÍNTESE DO PROJETO



Data de início: 2015-10-01 Data de fim: 2017-12-31

### DESIGNAÇÃO - Melhoria da Gestão da Segurança da Informação e dos Serviços da Função Informática no Ministério da Saúde

#### ➤ SUB-PROJETO A - Gestão do Risco e da Segurança do Sistema de Informação da Saúde

ATIVIDADES  
SUB-PROJETO A

- Estabelecer orientações com os requisitos mínimos para Política da Segurança da Informação a adotar por todas as entidades do Ministério da Saúde
- Estruturar o circuito para o registo de incidentes de segurança
- Produzir matéria para promover e sensibilizar a importância da segurança de informação nos Sistemas de Informação da Saúde
- Encetar iniciativas de auditoria à utilização da Política de Segurança com base na ISO 27799



#### ➤ SUB-PROJETO B - Gestão dos Serviços do Sistema de Informação da Saúde

ATIVIDADES  
SUB-PROJETO B

- Promover e sensibilizar a adoção de boas práticas em alinhamento com a Framework ITIL V3 - Foundation
- Elaborar um catálogo de serviços IT



## A CONFORMIDADE GLOBAL NO SNS



- Implementar uma metodologia transversal e estruturada entre as entidades que integram o SNS, que garanta a proteção, ao nível da Cibersegurança, dos Sistemas de Informação/ Tecnologias de Informação e equipamentos médicos, para impedir a utilização indevida ou perniciosa e o roubo de informação
- Definir objetivos estratégicos, eixos de intervenção e linhas de ação para materialização da metodologia a adotar
- Capacitar as entidades do SNS na deteção e resposta a incidentes de Cibersegurança
- Promover nas entidades do SNS um processo de melhoria contínua nível da Cibersegurança
- Garantir a conformidade com os preceitos legais de Cibersegurança



# IMPLEMENTAÇÃO DE UMA METODOLOGIA TRANSVERSAL E ESTRUTURADA - FUNDAMENTOS

- Conquanto, o processo de conformidade, em termos conceptuais, ser um objetivo transversal ao universo do SNS, é imperativo ter em consideração as vicissitudes específicas e distintivas de cada entidade *per si*;
- Consequentemente, o processo de conformidade no âmbito da Cibersegurança, do ponto de vista da implementação, requer que a sua execução seja efetuado, *in situ*, ou seja, em cada uma das entidades do SNS;
- No entanto, os denominadores comuns são essenciais de forma a estruturar um processo que articule e permita os mesmos objetivos, conceitos, níveis de conhecimento e estrutura de informação e que, motive, a partilha de conhecimento entre as entidades;
- Assim, permitirá desenvolver um processo de conformidade simbiótico (contribuir para a implementação de sinergias e relações de cooperação entre os organismos) que permitirá evoluir, numa fase posterior, para um contexto federado, de forma a poder otimizar os custos subjacentes ao nível dos recursos especializados no âmbito da Cibersegurança.





# DEFINIÇÃO DOS OBJETIVOS ESTRATÉGICOS E EIXOS DE INTERVENÇÃO



- Conceção de um plano de ação, para materialização da metodologia transversal e estruturada, cujo objetivo é agilizar a capacidade das entidades, que integram o SNS, ao nível da Cibersegurança, através de objetivos estratégicos (OE) e correspondentes eixos de intervenção (EI):

- EI 1: Inventariar os Sistemas de Informação/Sistemas/Aplicações, os equipamentos médicos, os ativos tangíveis e não tangíveis, os responsáveis e os prestadores de serviço correspondentes, bem como, o enquadramento, no contexto da legislação de proteção de dados, ao nível do tratamento de dados
- EI 2: Classificar os Sistemas de Informação/Sistemas/Aplicações ao nível da criticidade detalhando a sua relação com os ativos tangíveis e não tangíveis, bem como, os responsáveis e os prestadores de serviço correspondentes
- EI 3: Criar capacidade para deteção e resposta a incidentes, ou seja, a operacionalização de um *Security Operation Center* (SOC), que deve obedecer às seguintes linhas de ação:
  - EI 3.1: Garantir aos meios tecnológicos de base ao SOC e os recursos humanos necessários e especializados para a respetiva instalação, configuração e manutenção
  - EI 3.2: Assegurar os recursos humanos para a monitorização dos incidentes de Cibersegurança e operacionalizar os serviços e processos adjacentes
- EI 4: Assegurar a obtenção da Certificação do Selo de Maturidade Digital na dimensão Cibersegurança
  - EI 4.1: Avaliar a conformidade no Contexto do Selo de Maturidade Digital na dimensão Cibersegurança
  - EI 4.2: Certificar a Organização no Selo de Maturidade Digital na dimensão Cibersegurança
- EI 5: Garantir um processo de continuidade e melhoria contínua dos Eixos de Intervenção

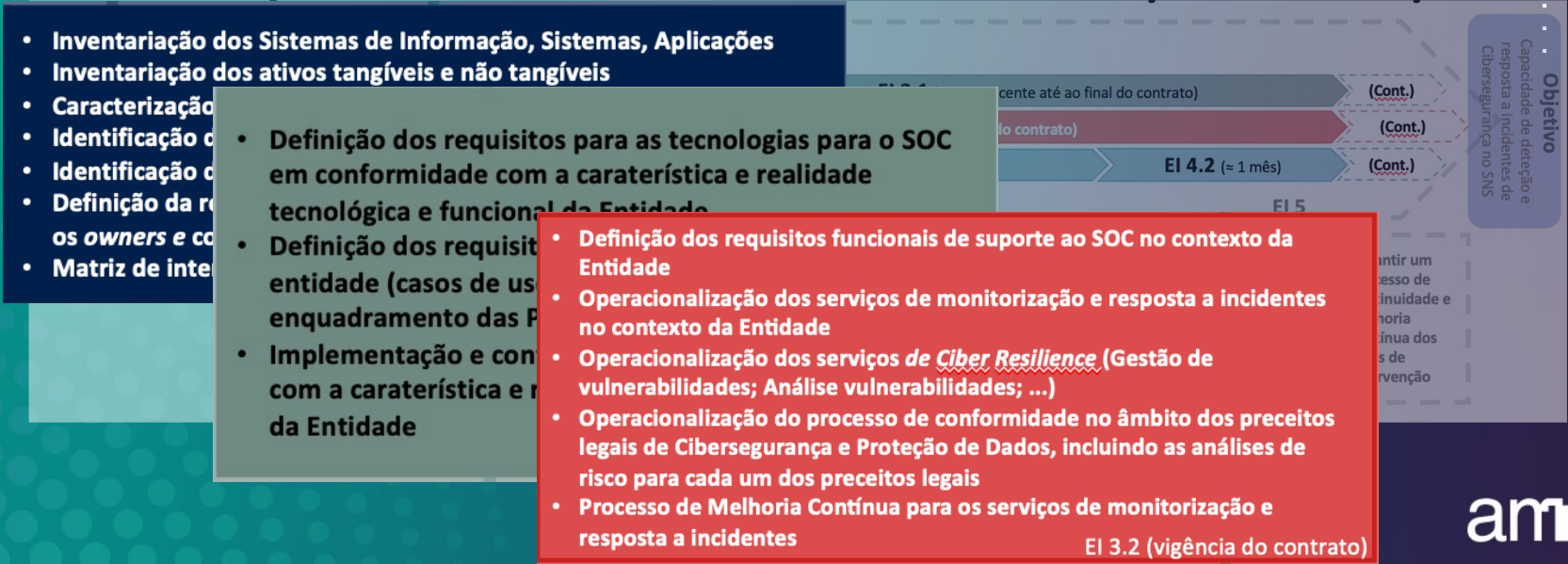
- OE 1: Garantir a conformidade com os Preceitos Legais de Cibersegurança
- OE 2: Garantir e consolidar a capacidade de Cibersegurança do SNS
- OE 3: Garantir a certificação Selo de Maturidade Digital na dimensão Cibersegurança
- OE 4: Garantir a continuidade e melhoria contínua



# CRONOGRAMA TEMPORAL DOS EIXOS DE INTERVENÇÃO & LINHAS DE AÇÃO



- Capacitar as entidades do SNS na deteção e resposta a incidentes de Cibersegurança;
- Promover nas entidades do SNS um processo de melhoria contínua nível da Cibersegurança;
- Garantir a conformidade com os preceitos legais de Cibersegurança.



- EI 1: Inventariar os Sistemas de Informação/Sistemas/Aplicações, os equipamentos médicos, os ativos tangíveis e não tangíveis, os responsáveis e os prestadores de serviço correspondentes, bem como, o enquadramento, no contexto da legislação de proteção de dados, ao nível do tratamento de dados
- EI 2: Classificar os Sistemas de Informação/Sistemas/Aplicações ao nível da criticidade detalhando a sua relação com os ativos tangíveis e não tangíveis, bem como, os responsáveis e os prestadores de serviço correspondentes
- EI 3: Criar capacidade para deteção e resposta a incidentes, ou seja, a operacionalização de um *Security Operation Center* (SOC), que deve obedecer às seguintes linhas de ação:
  - EI 3.1: Garantir aos meios tecnológicos de base ao SOC e os recursos humanos necessários e especializados para a respetiva instalação, configuração e manutenção
  - EI 3.2: Assegurar os recursos humanos para a monitorização dos incidentes de Cibersegurança e operacionalizar os serviços e processos adjacentes
- EI 4: Assegurar a obtenção da Certificação do Selo de Maturidade Digital na dimensão Cibersegurança
  - EI 4.1: Avaliar a conformidade no Contexto do Selo de Maturidade Digital na dimensão Cibersegurança
  - EI 4.2: Certificar a Organização no Selo de Maturidade Digital na dimensão Cibersegurança
- EI 5: Garantir um processo de continuidade e melhoria contínua dos Eixos de Intervenção



**OBRIGADO**

