

Caminho dos Hospitais

Os Desafios da Cibersegurança na Saúde

Instituto Português de Oncologia de Coimbra
11h, 4 de dezembro de 2017

APAH
ASSOCIAÇÃO PORTUGUESA
DE ADMINISTRADORES HOSPITALARES



SPMS EPE
Serviços Partilhados do
Ministério da Saúde

Dezembro de 2017
IPO Coimbra

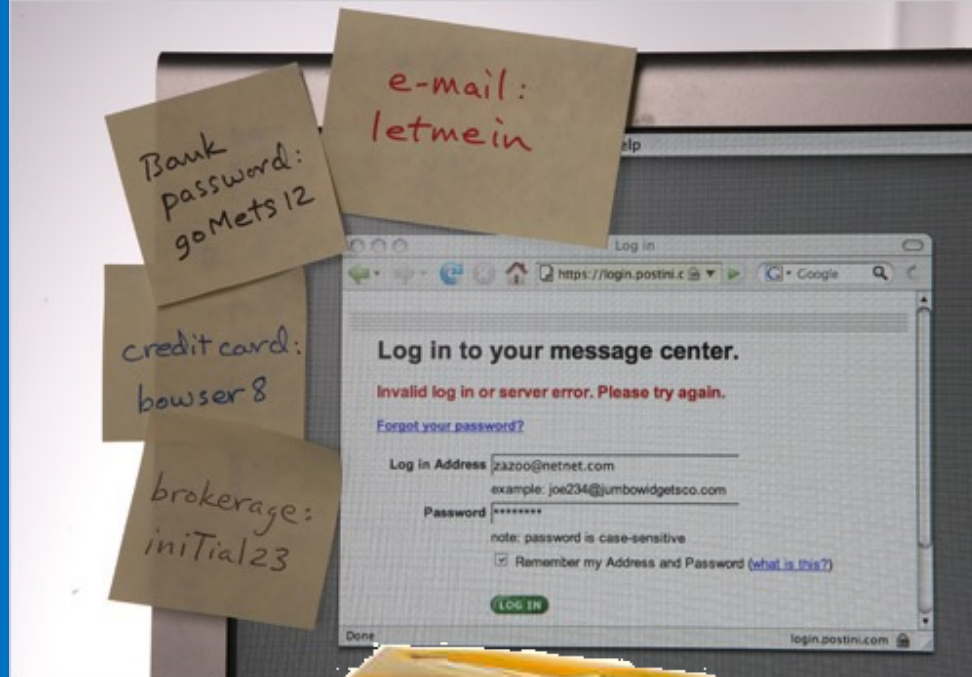
Desafios da cibersegurança

Professor Henrique Martins | Presidente do CA
Serviços Partilhados do Ministério da Saúde

Segurança



Realidade...



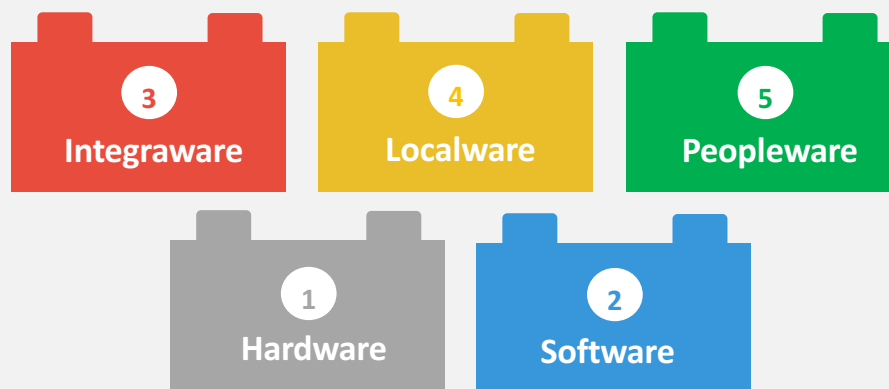


SPMS^{EPE}
Serviços Partilhados do
Ministério da Saúde



Resolução de Conselho de Ministros nº62/2016

Estratégia Nacional para o Ecosistema de Informação de Saúde 2020



SNS SERVIÇO NACIONAL
DE SAÚDE



Resolução de Conselho de Ministros nº62/2016

Estratégia Nacional para o Ecosistema de Informação de Saúde 2020

- ✓ Gestão da mudança e promoção das competências dos recursos humanos
- ✓ Arquitetura de sistemas abrangente, comunicável e auditável
- ✓ Melhoria da segurança da informação e usabilidade
- ✓ Atualização do parque informático e dos sistemas legados
- ✓ Acesso da informação pelo cidadão em omni-canal
- ✓ Transparência e interoperabilidade
- ✓ Utilização de informação para melhoria da saúde
- ✓ Partilha de recursos
- ✓ Tele saúde e desmaterialização



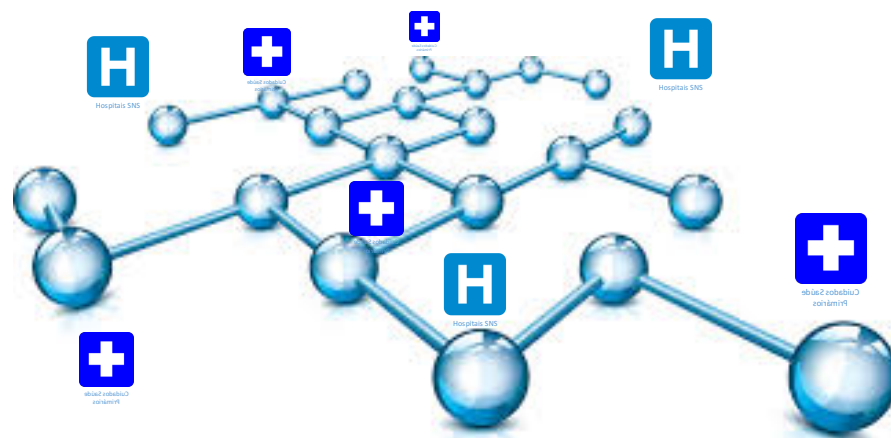
491

Instituições de CSP

76

Hospitais

Plataforma de Dados da Saúde



- Utente
- Representantes Institucionais
- Profissionais de Saúde Habilitados
- Profissionais de Saúde Estrangeiros Habilitados
- Funcionários Administrativos de Saúde



 **SNS** SERVIÇO NACIONAL
de SAÚDE

 **ÁREA** do
CIDADÃO

Se conhece o Portal do SNS? Num único local, toda a informação de saúde.
Acede e regista-se na Área do Cidadão.
Podes registar consultas, receber notificação de exames, visualizar o teu plano de tratamento, entre
outras funcionalidades.
Vais sempre a par do SNS: www.sns.gov.pt

Nova Área do Cidadão do Portal SNS
Acompanha a tua Saúde



Acede com

[Esqueceu-se da palavra-passe?](#)

Também pode aceder
com o Cartão de Cidadão/Chave Móvel Digital



Ainda não se registou?
É rápido e simples.

Área do Cidadão

www.sns.gov.pt/cidadao

O que fizemos?

PDS Live

Telemedicina – princípios básicos

- Total mobilidade, todos os gabinetes médicos para todos os profissionais
- Multiplataforma / Multidevice
- Fornecedor-independente
- Sem custos de manutenção externos



Cuidados de Saúde primários

+13.000 profissionais

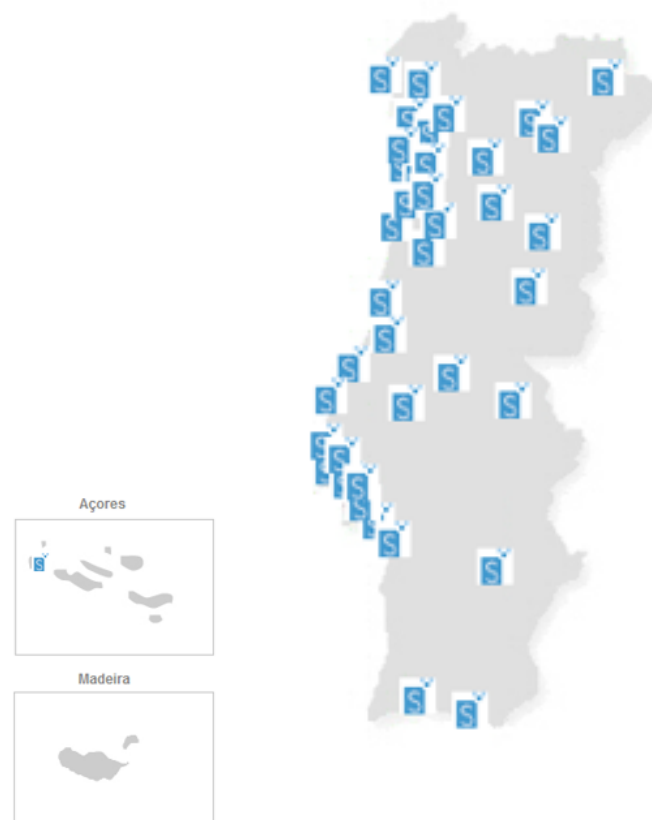
+300 entidades



Hospitais

+60.000 profissionais

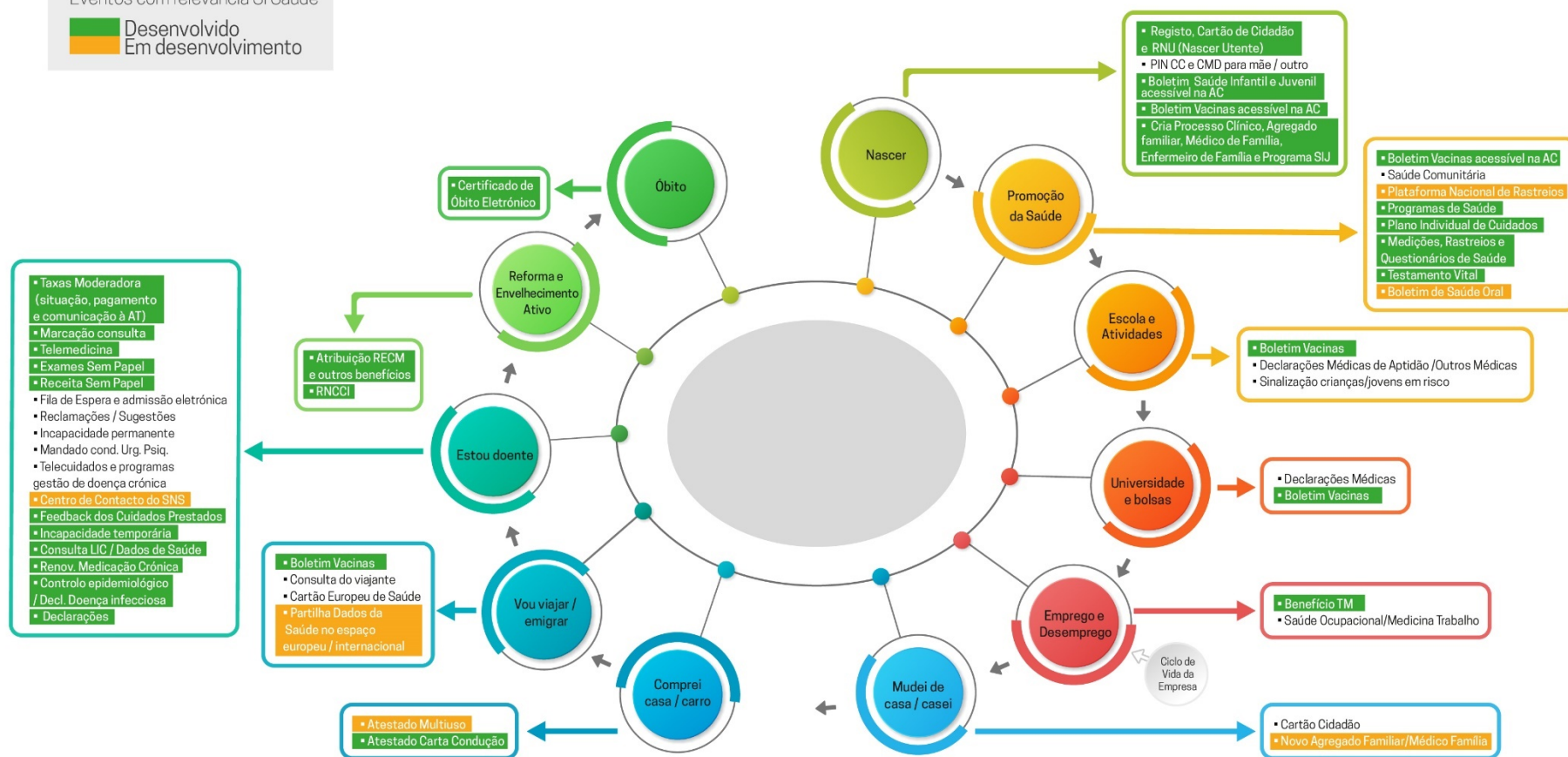
+50 entidades



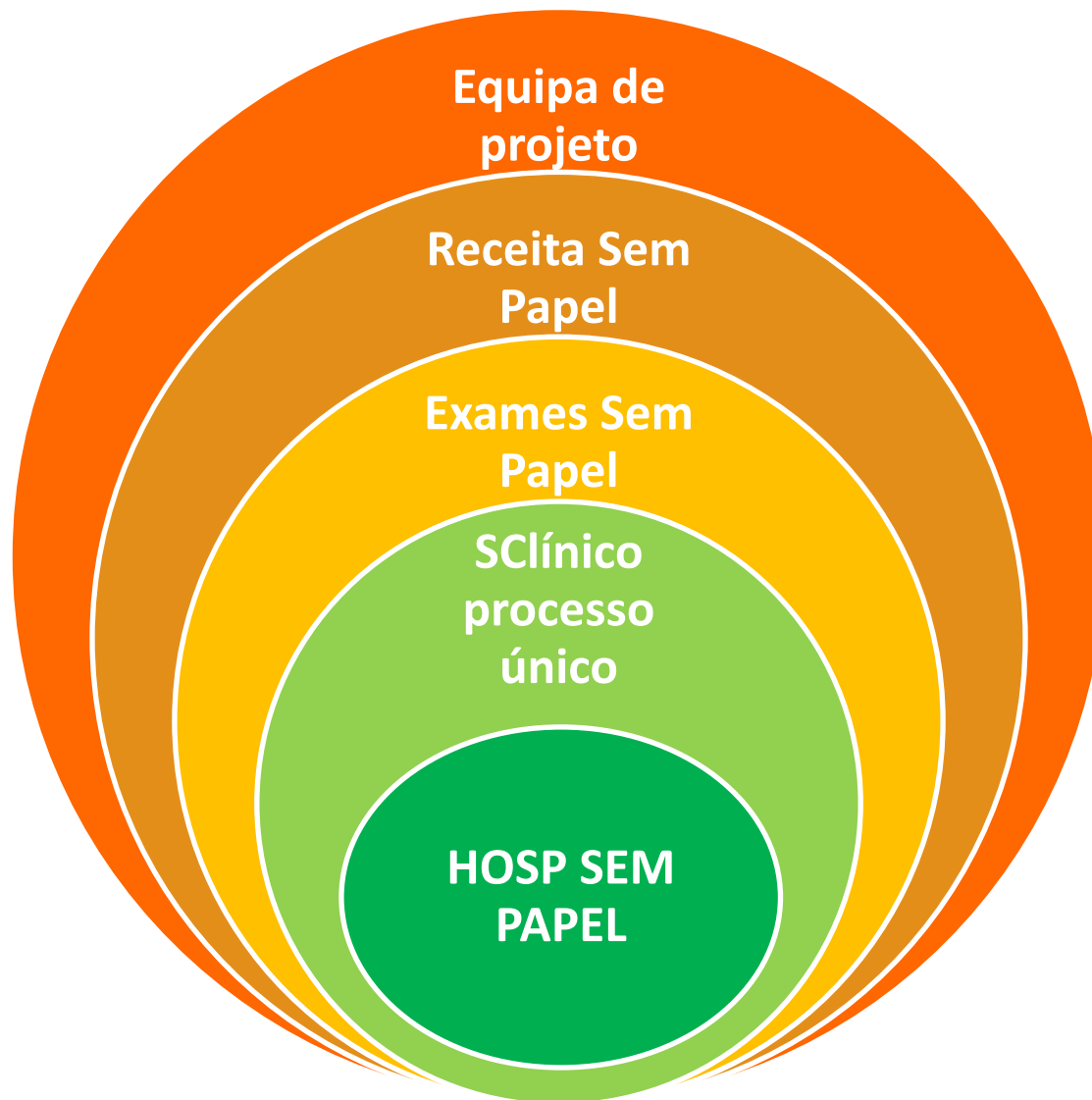
CICLO DE VIDA DO CIDADÃO

Eventos com relevância SI Saúde

Desenvolvido
Em desenvolvimento



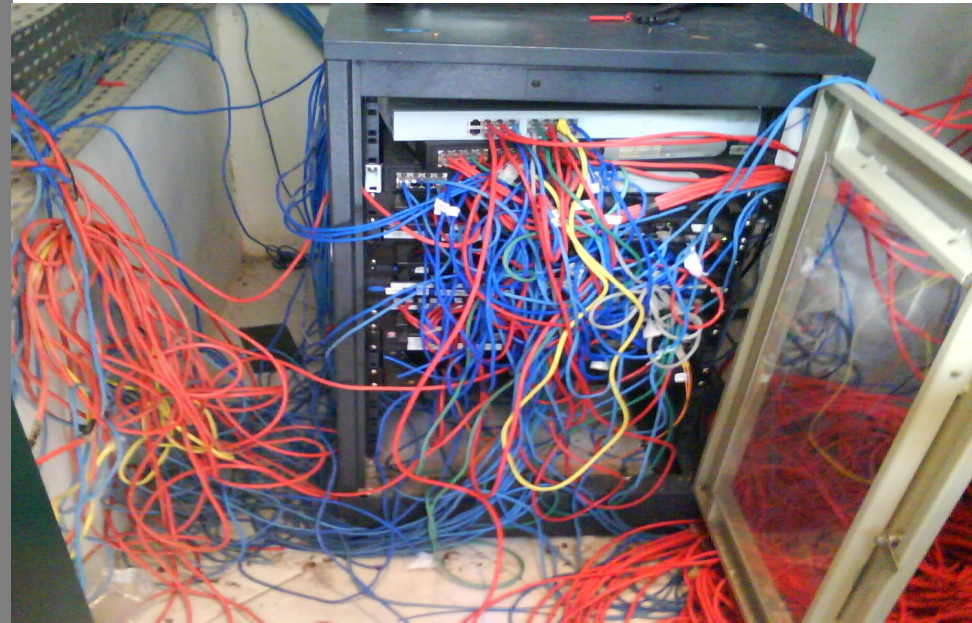
Programas Piloto Hospitalais SEM PAPEL





SPMS^{EPE}
Serviços Partilhados do
Ministério da Saúde

Mito ou realidade?
Hardware



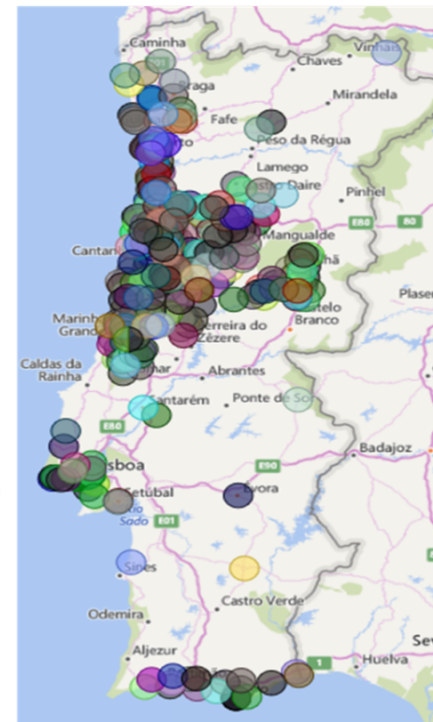
Aumento
capacidade da rede

Substituição
computadores obsoletos

Número de Instituições com planeamento

478

Intervenção	Contagem de Institui...	% Realização
Em avaliação	46	0%
4Mbps - 8Mbps	6	83%
300Mbps - 600Mbps	1	100%
2Mbps - 4Mbps	252	81%
2Mbps - 10Mbps	4	50%
20Mbps - 40Mbps	1	100%
10Mbps - 20Mbps	156	98%
10Mbps - 100Mbps	3	100%
100Mbps - 200Mbps	9	67%
Total	478	78%



Mito ou realidade? Interoperabilidade e Arquitetura





INTEROPERABILIDADE

QUAL A ESTRATÉGIA SPMS ?

Arquitetura de Sistemas
de Informação para a Saúde



Alinhament

Integração

Mudança

Rapidez e
Eficiência

Arquitetura do Negócio

Arquitetura da Informação

Arquitetura Aplicacional

Arquitetura Tecnológica

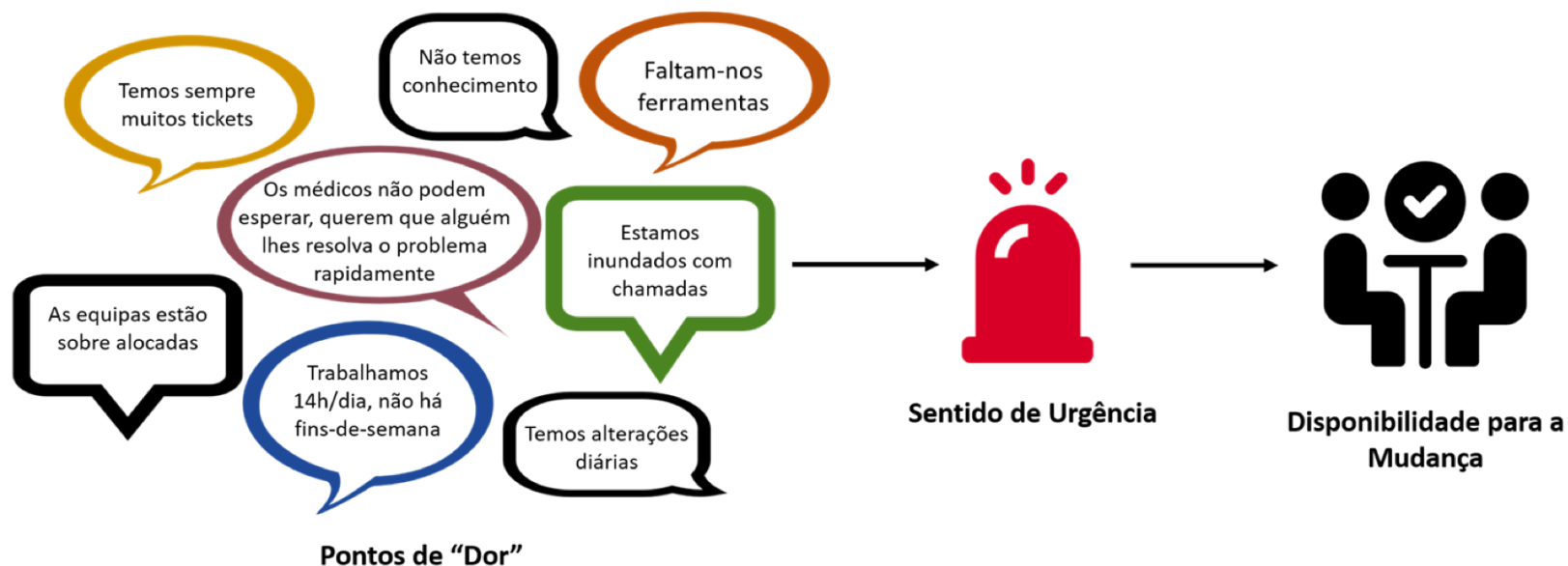
Motivação

- Redução Custos
- Aumento da Coerência da Informação
- Alinhamento do Negócio com TI
- Redução de Risco
- Apoio à Mudança
- Promoção da Interoperabilidade
- Facilitar o Acesso à Informação
- Segurança de Informação
- Gestão de Contratos
- Gestão de Serviços

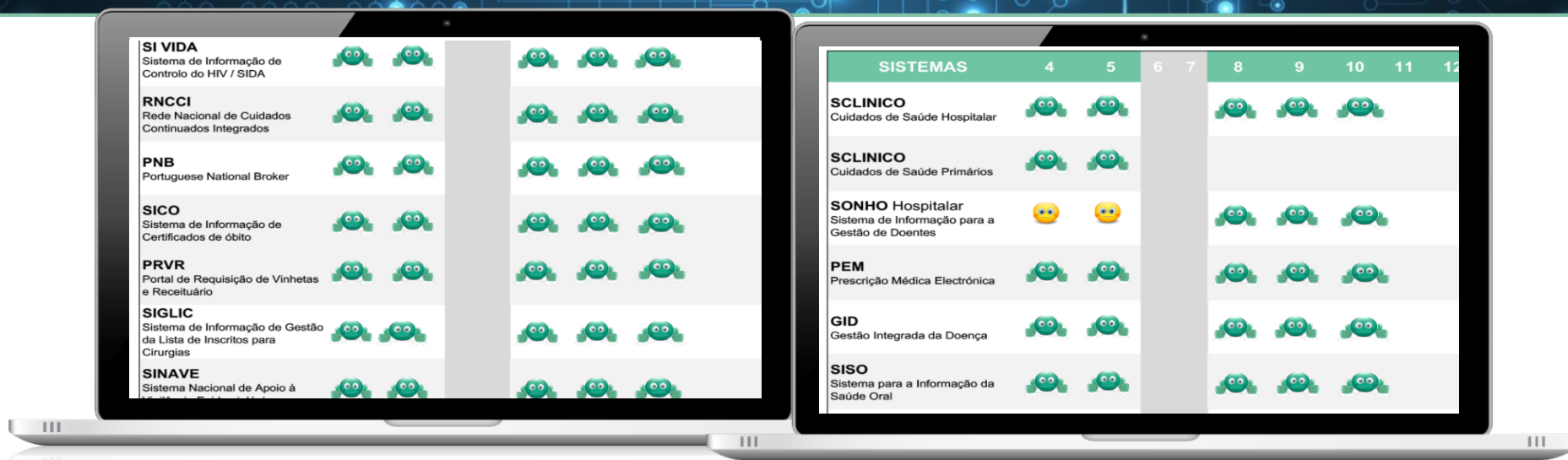
Mito ou realidade? Suporte



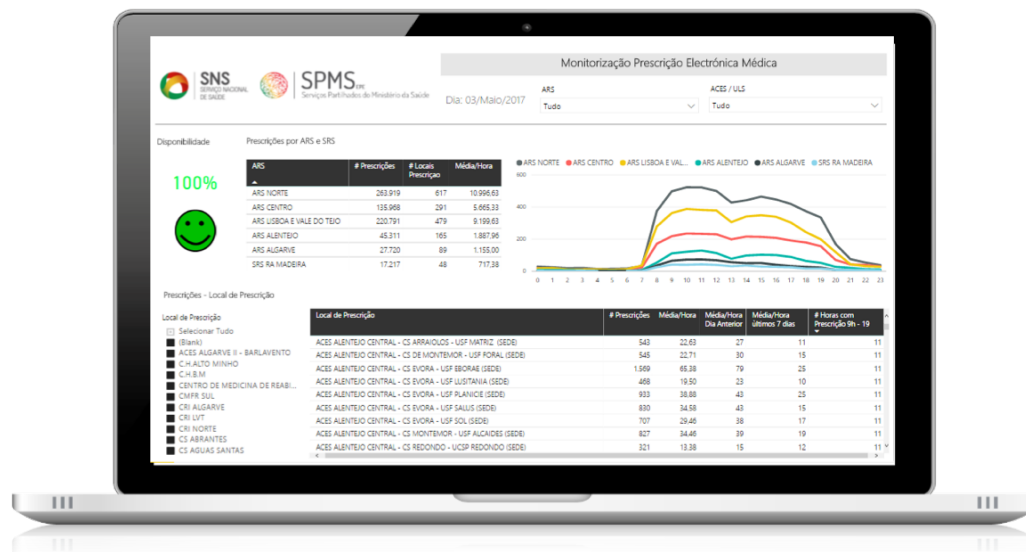
Porquê um Modelo de Gestão de Serviço e Suporte (MoGSS)?



MONITOR DOS SISTEMAS DE INFORMAÇÃO DA SPMS



MONITOR DOS SISTEMAS DE INFORMAÇÃO DA SPMS



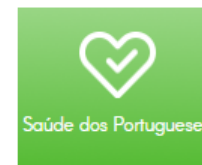
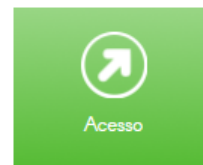
Mito ou realidade?

Transparência SNS



127

Datasets







SPMS^{EPE}
Serviços Partilhados do
Ministério da Saúde

Mito ou realidade?

Apps



87%

Dos utilizadores de
internet têm um
smartphone





• Rede Informática da Saúde





Novo sistema de email no SNS

- ▶ Acessível em qualquer lugar
- ▶ Design mais intuitivo e atrativo
- ▶ Mais espaço de armazenamento
- ▶ Sistema de segurança de informação de última geração



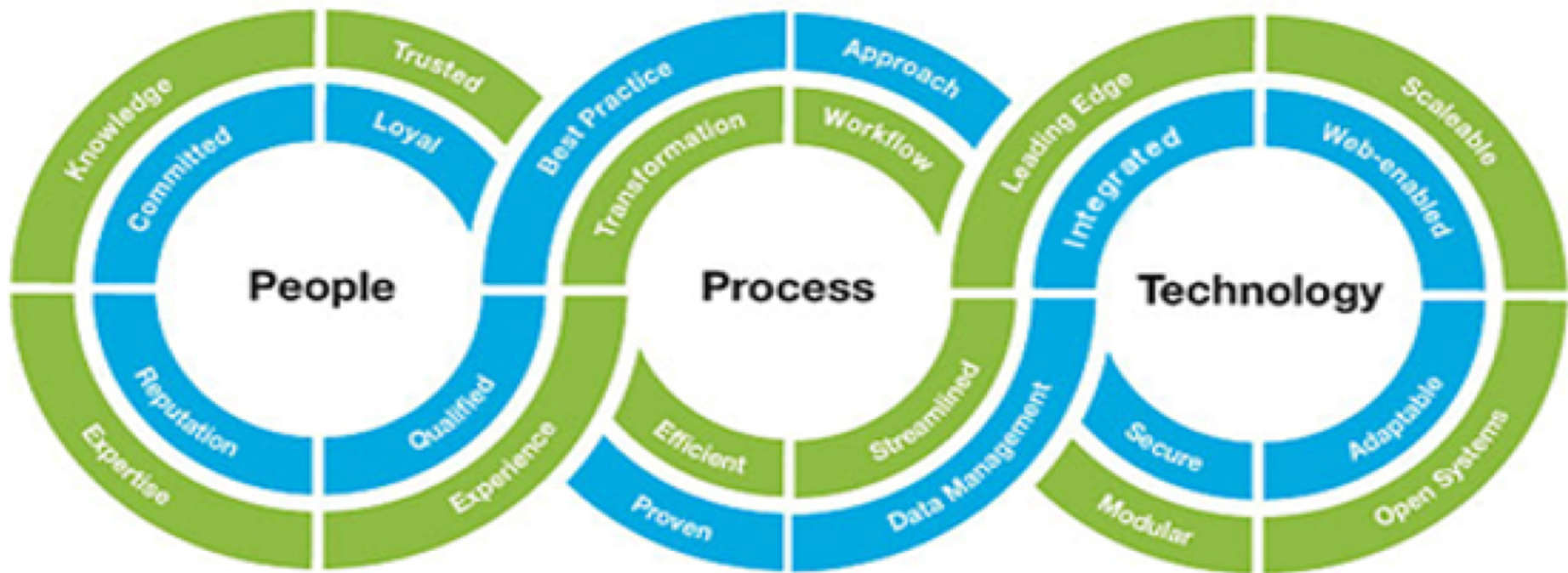
Migrado

105788

Target: 120.000

Realidade...

Programa de Melhoria Contínua do Risco e Segurança da Informação



Segurança



Segurança em eHealth
Proteção do Hospital do futuro

15 de novembro

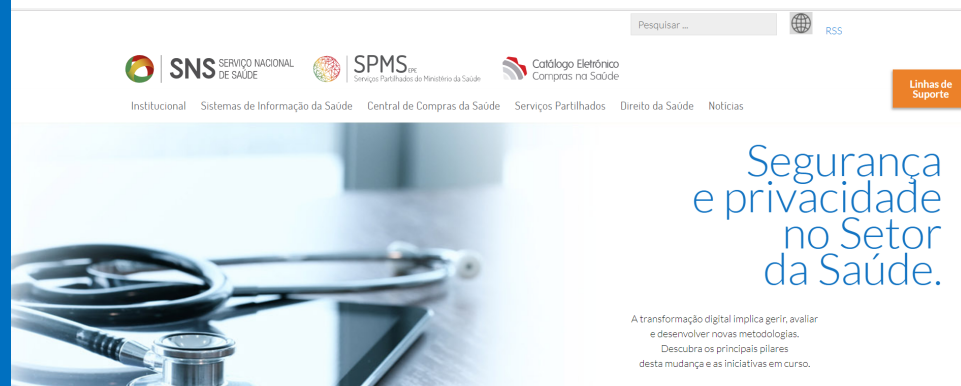
Lisboa

Auditório da Faculdade de Medicina Dentária
Universidade de Lisboa

3rd eHealth Security Conference
Protecting the Hospital of tomorrow

Segurança

SPMS IT security assessment



INICIATIVAS SPMS

- Programa de Segurança de Informação e Privacidade no Setor da Saúde em Portugal;
- Boas práticas de Segurança e Privacidade da informação no setor da Saúde;
- RGPD – Implicações para as entidades do setor da Saúde.

**Circular
Informativa
n.º1 de 2017
da SPMS
15 de
fevereiro**

**Protocolo de
Cooperação
entre o
GNS/CNCS
e a SPMS
21 de
fevereiro
2017**

**Estratégia de
Cibersegurança
da Saúde

Canais de
Comunicação**

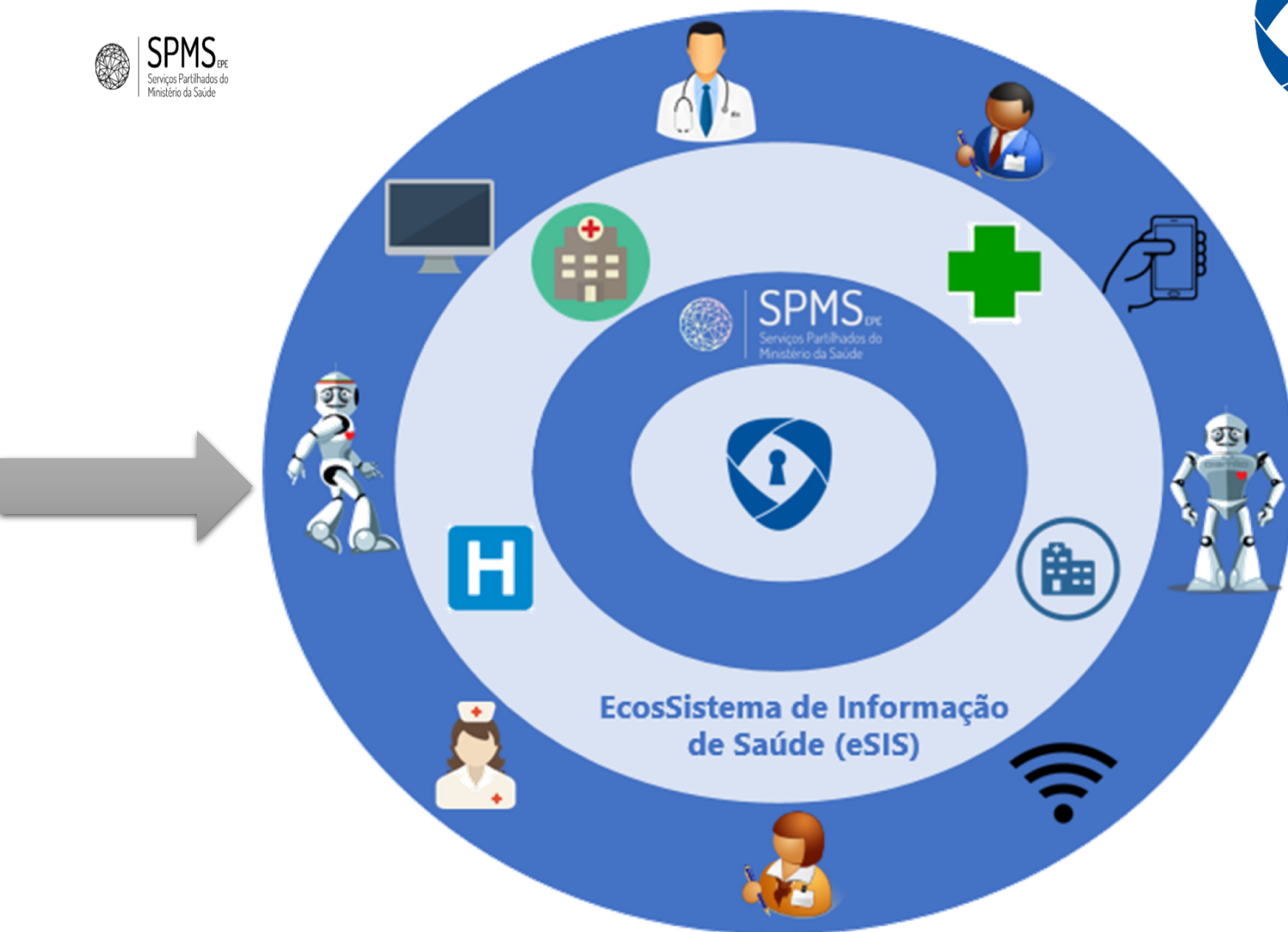
**Medidas
Excecionais de
Cibersegurança
Circulares
Normativas
n.º 1 a n.º 4 e
n.º 7**

**Resolução do
Conselho de
Ministros
nº 62/2016
17 de outubro
ENESIS 2020**

**Despacho
n.º 1348/2017
8 de fevereiro**

**Resolução do
Conselho de
Ministros
n.º 115/2017
24 de agosto**

**Despacho
n.º 8877/2017
9 de outubro**



Plano de Ação de Segurança da Informação alinhado com o Plano Estratégico da SPMS, EPE

16 Iniciativas

Status

❖ Identificação dos compromissos e atividades de segurança assumidos pelo PE	100%
❖ Definição do âmbito de proteção das iniciativas de Segurança da Informação	100%
❖ Adaptação da Política de Segurança da informação existente	100%
❖ Adoção da Unidade Orgânica para Gestão da Segurança da Informação	100%
❖ Adoção do modelo de Comunicação para Gestão da Segurança da Informação	50%
❖ Adoção de processos de gestão Segurança, Políticas e Procedimentos	50%
❖ Identificação da conformidade legal aplicável e normas internacionais a cumprir	Em curso
❖ Criação do inventário dinâmico de recursos do âmbito de proteção (Arquitetura)	Em curso
❖ Elaboração de um Protótipo de Análise de Risco de serviços críticos	100%
❖ Identificação de vulnerabilidades, ameaças e riscos associados a ativos	Em curso
❖ Implementação de Requisitos de Segurança de Informação em Sistemas	Em curso
❖ Adoção de um Sistema de Registo de Incidentes de Segurança da Informação	60%
❖ Adoção de um Sistema de Gestão de Identidades na SPMS	Em curso
❖ Implementação de um <i>Disaster Recover</i> (Serviços Redundantes)	Em curso
❖ Adoção de Procedimentos para Continuidade de Negócio	Em curso
❖ Implementação de um Sistema de Gestão de Risco e Segurança	Em curso

Cibersegurança na Saúde

Cooperação e Iniciativas no âmbito do eSIS

- ***Despacho n.º 1348/2017 de 8 de fevereiro*** do Secretário de Estado da Saúde Estabelece a Notificação Obrigatória Centralizada de Incidentes de Segurança no SNS/MS_ Nomeação de RNOs.
- ***Medidas Excepcionais de Cibersegurança*** _ Depois de ***12 de maio de 2017***
 - ***Circulares normativas*** n.º 1; n.º 2; n.º 3; n.º 4; n.º 7
 - ***Termo de Compromisso Institucional para a Cibersegurança na Saúde*** _ 70% das Entidades SNS/MS assinaram com a SPMS o documento.
- ***Despacho n.º 8877/2017 de 9 de outubro*** do Secretário de Estado da Saúde Estabelece o Modelo de Governação relativo à implementação da Política de Cibersegurança da Saúde
- ***1.ª Iniciativa de Avaliação do âmbito da Segurança da Informação***
Participaram 17 Entidades nas componentes de Conformidade e Técnica
- ***Iniciativas #1 e #2 de Ativação de Boas Práticas de Segurança da Informação no eSIS***
- ***Divulgação do Flyer de Segurança da Informação***

Reporte de incidentes

24 incidentes
reportados desde
nov 2016

~2 incidentes por
mês

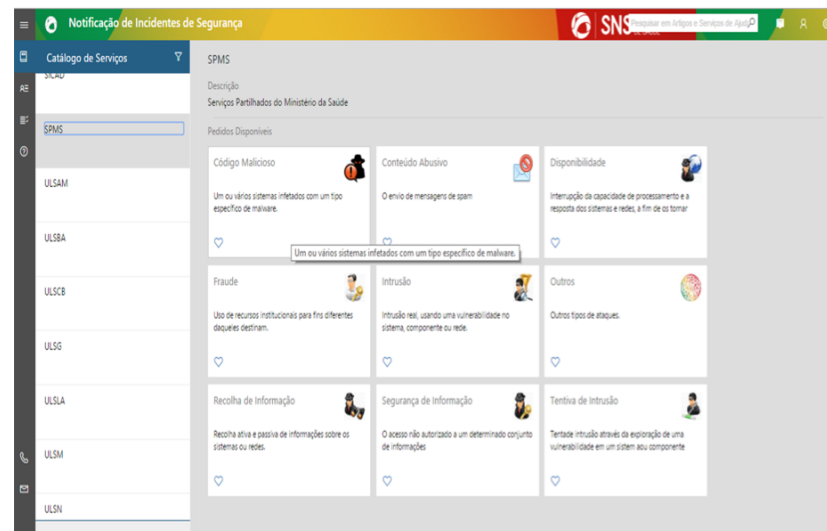
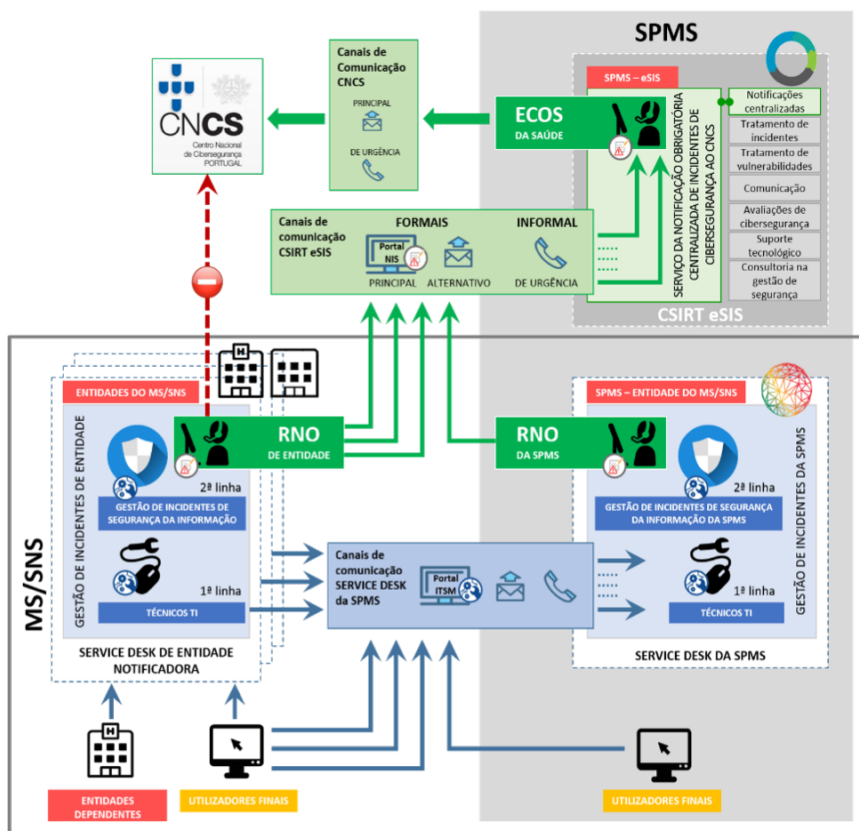
- Política de Segurança da Informação
- Framework da Documentação no Âmbito da Segurança da Informação
- Glossário de Segurança da Informação
- Management of logical access control

Boas práticas na SPMS...
não somos os melhores, mas
queremos ser



Boas Práticas de Segurança da Informação no eSIS

Notificação obrigatória Centralizada de Incidentes de segurança

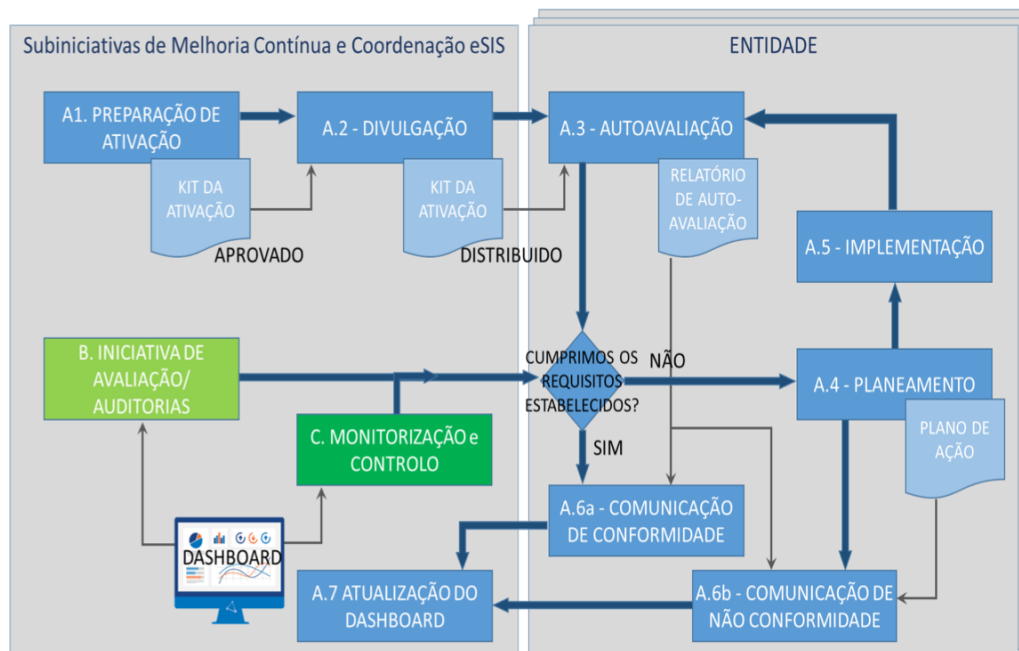


Plataforma de Notificação de Incidentes de Segurança NIS

Processo de Notificação

Boas Práticas de Segurança da Informação no eSIS

Visão geral do “Processo de Ativação de Práticas no eSIS” e Iniciativas relacionadas



✓ Ativação # 1 _ 22.06.2016

- **KIT 1** Framework de Referência do Risco e Segurança da Informação;
- **KIT 2** Framework da Documentação no Âmbito da Segurança da Informação;
- **KIT 3** Princípios de Segurança da Informação;
- **KIT 4** Objetivos de Segurança da Informação;
- **KIT 5** Política de Segurança da Informação.

✓ Ativação # 2 _ 10.03.2017

Suporte à avaliação implementação de controlos de Cibersegurança:

- **CCS 8** _ Defesas de Malware;
- **CCS 10** _ Recuperação de Dados;
- **CCS19** _ Resposta e Gestão de Incidentes.

Boas Práticas de Segurança da Informação no eSIS

Serviço de Auditorias e Avaliação do eSIS

✓ *1.ª Iniciativa (fev. – abr. 2017)*

✓ *17 Entidades*

✓ *Componentes:*

- *Técnica (pen testing);*
- *Conformidade (questionário online)*



Protocolo de Cooperação no âmbito do Programa da Cibersegurança da Associação Nacional de Farmácia (ANF) com a SPMS





SPMS^{EPE}
Serviços Partilhados do
Ministério da Saúde

Protocolo de Cooperação entre a SPMS através da Academia de Formação e o CHUC para a criação do Centro de Desenvolvimento e Capacitação da Cibersegurança



SPMS^{EPE}
Serviços Partilhados do
Ministério da Saúde



ACADEMIA SPMS
qualificação & inovação



CHUC
CENTRO HOSPITALAR
E UNIVERSITÁRIO
DE COIMBRA

PROTOCOLO DE COOPERAÇÃO

Framework Agreement of Cybersecurity

Category I – Security Government and Risk Management

- Lot 1 – Security strategy and plan of action
- Lot 2 – Risk analysis
- Lot 3 – Security policies and standards
- Lot 4 – Performance evaluation
- Lot 5 – Continuity management
- Lot 6 – Conformity

Category II – Security Threat Management

- Lot 7 – Definition of the implementation plan of a security operation center (SOC)
- Lot 8 – Implementation of a security operation center (SOC)
- Lot 9 – Definition of the monitoring model for a security operation center (SOC)
- Lot 10 – Operation of a security operation center (SOC)
- Lot 11 – Security threat identification and evaluation
- Lot 12 – Incident management/response definition
- Lot 13 – Incident response service

Framework Agreement of Cybersecurity

Category III – Security Engineering

- Lot 14 – Physical security
- Lot 15 – Design of network architectures and secure communications
- Lot 16 – Implementation and administration of network architectures and secure communications
- Lot 17 – Security in the software development cycle

Category IV – Identity and Access Management

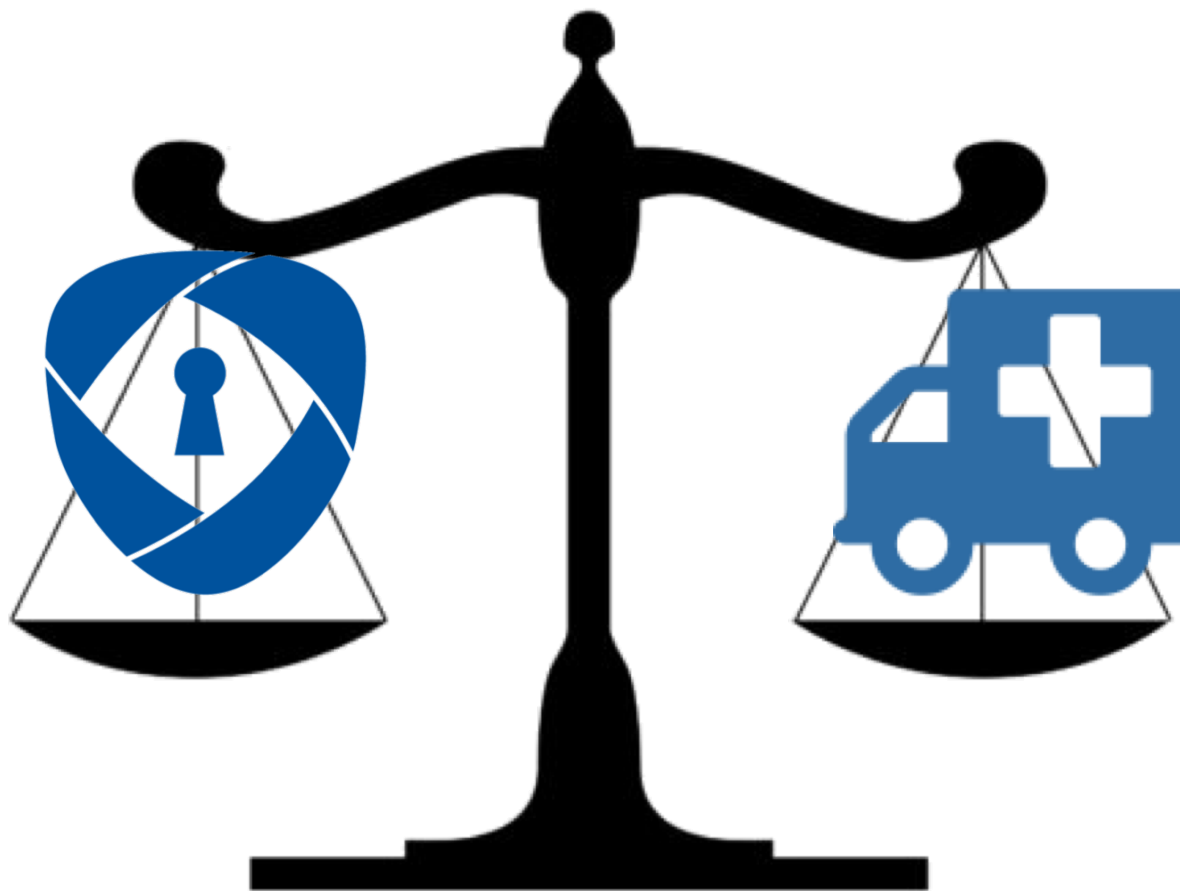
- Lot 18 – Elaboration of access policies
- Lot 19 – Entity management and logical access control

- Lot 20 – Implementation of the identity and access management process
- Lot 21 – Public keys infrastructures
- Lot 22 – Implementation of public keys infrastructures

Category V – Protection of Personal Data and Privacy

- Lot 23 – Strategy and government for protection of personal data
- Lot 24 – Classification and management of information
- Lot 25 – Protection against loss of information

Temos equilíbrio





Os 10 mandamentos da cibersegurança

**Não
introduzirás
pens alheias
no PC de
trabalho**

**Não deixarás o
teu PC
desbloqueado,
mesmo entre
amigos ou
colegas**

**Não
esquecerás
os backups e
apostarás na
redundância**

**Não desejarás
trabalhar fora de
ambientes e
redes seguras**

**Não
esquecerás o
antivírus**

**Não
cobiçarás
phishing
alheio**

**Assumirás o
papel de
melhor linha de
defesa contra
os ciberataques**

**Não partilharás
passwords
e códigos de
acesso**

**Amarás as
medidas de
segurança sobre
todas as coisas**

**Não
procrastinarás as
atualizações,
mesmo aos
domingos e
feriados**



SPMS^{EPE}
Serviços Partilhados do
Ministério da Saúde

Flyer cibersegurança



A SEGURANÇA DA INFORMAÇÃO

INFORMAÇÃO AO COLABORADOR

Novembro | 2017



Índice

Introdução	
Princípios gerais de segurança	
As passwords e o acesso à informação	
Posto de trabalho e salas de trabalho	
O correio eletrónico e NetEducação	
Phishing, vírus e ransomware	
A Internet e a comunicação	
Dispositivos móveis	
Parceiros externos	
GDPR	
Destruição de dados e impressão	
Segurança de pagamentos e cartões	
Dez Mandamentos de Segurança	



Glossário de segurança de informação



A		C	
Aceitação do risco	Decisão informada de aceitar um risco	Cavalo de Troia	Programa, normalmente recebido como um "presente" (e.g. cartão virtual, álbum de fotos, protetor de ecrã, jogo), que além de executar funções para as quais foi aparentemente projetado, também executa outras funções normalmente maliciosas e sem o conhecimento do utilizador. Vulgarmente chamado pelo termo em Inglês <i>Trojan Horse</i> .
Ação corretiva	Ação ou atividade que é planeada e executada para garantir a conformidade e prevenir a sua recorrência		
ADSL	Do Inglês <i>Asymmetric Digital Subscriber Line</i> . Tecnologia das linhas telefónicas para transmissão de dados em velocidades superiores às das linhas de voz.		
Adware	Ransomware	Código malicioso que restringe o acesso ao sistema infetado e cobra um valor de "resgate" para que o acesso possa ser reestabelecido.	
	Rede sem fios	Rede que permite a conexão entre computadores e outros dispositivos através da transmissão e receção de sinais de rádio. Vulgarmente chamado pelo termo em Inglês <i>Wireless</i> .	
	Responsável (<i>Responsible</i> no modelo RACI)	Aqueles que fazem o trabalho para realizar a atividade ou tarefa. Há pelo menos um papel com um tipo de participação de "Responsável", embora outros possam ser delegados para auxiliar no trabalho exigido.	
Ameaça			
Análise de riscos	Risco	A combinação de consequências de um determinado evento ao qual está associada uma probabilidade de ocorrência.	
Antivírus	Risco residual	Risco remanescente após o tratamento do risco inerente.	
	Rootkit	Conjunto de programas que tem como finalidade esconder e assegurar a presença de um invasor num computador comprometido. É importante referir que o nome <i>rootkit</i> não indica que as ferramentas que o compõem sejam usadas para obter acesso privilegiado (<i>root</i> ou <i>Administrator</i>) num computador, mas sim para ocultar a presença do invasor.	

Um convite

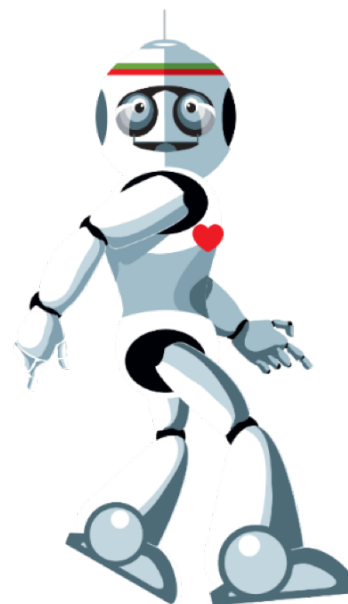




SPMS^{EPE}
Serviços Partilhados do
Ministério da Saúde

Dezembro de 2017
IPO Coimbra

A solução está na partilha!



Professor Henrique Martins | Presidente do CA
Serviços Partilhados do Ministério da Saúde