A Cibersegurança, visão do Estado

Manuel Honorato
CMG
Eng.º de Material Naval

Sumário

- Plano Global Estratégico de Racionalização e Redução de Custos nas TIC, na Administração Pública (PGERRCTIC)
- Centro de Gestão da rede Informática do Governo (CEGER) como Prestador de Serviços
- Conclusões

Enquadramento

- **RCM n.º 46/2011 – Criação do Grupo para as Tecnologias de Informação e Comunicação (GPTIC)**

- **RCM n.º 12/2012 – Plano Global Estratégico de Racionalização e Redução de Custos nas TIC, na Administração Pública (PGERRCTIC)**
  - **25 Medidas**
  - **5 Vetores**
  - **Período de Implementação 2012-2016**
  - **Poupança estimada ~ 500 M€ / ano**

- **RCM n.º 60/2012 - Reestruturação do GPTIC**
  - **Comissão de Execução do GPTIC**
  - **Conselho Consultivo do GPTIC**
  - **Comité Técnico do GPTIC**

Medida 04 – Definição e Implementação de uma Estratégia Nacional de Segurança da Informação - Objetivos

- ***Os Objetivos Nacionais para a Segurança da Informação*** *– Aquilo que cada membro da Sociedade da Informação pode esperar e contar a nível nacional;*
- ***A Responsabilidade na Segurança da Informação*** *– Quem é responsável pela implementação da Segurança da Informação no país;*
- ***Organização da Segurança da Informação –*** *Qual a estrutura definida para a Segurança da Informação;*
- ***Gestão*** *– Quem é responsável por Estabelecer, Controlar e Medir, Gerir o Risco e Auditar a Segurança da Informação;*
- ***Serviços de Segurança da Informação –*** *Que serviços são fornecidos a nível nacional e por quem.*

Medida 04 – Definição e Implementação de uma Estratégia Nacional de Segurança da Informação - Ações

- **Estrutura Nacional de Segurança da Informação** – Revisão e promulgação;
- **Centro Nacional de Cibersegurança (CNCSeg) –** criação, instalação e operacionalização de Centro;
- **Sistema de Certificação Eletrónica do Estado (SCEE)** – aprofundamento e melhoria das condições de operação da SCEE, com vista à sua adequação aos requisitos internacionais mais recentes;
- **Criptografia Nacional** – criação e certificação de uma solução de criptografia forte de origem nacional, desenvolvimento de soluções para a sua utilização e promoção junto dos potenciais utilizadores;
- **Revisão do Quadro Legal para a Segurança das Matérias Classificadas** - incluindo a salvaguarda da informação classificada, da credenciação pessoal e industrial e ainda da segurança dos sistemas de comunicação e informação, substituído os SEGNAC's.

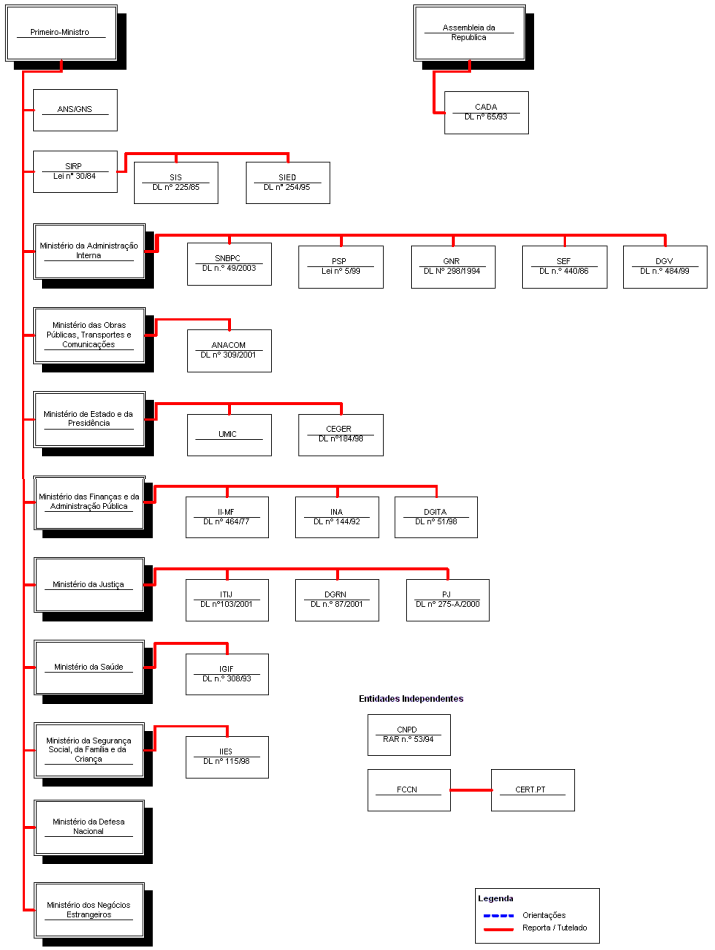
Elaboração Inicial da ENSI

- **UMIC** – Unidade de Missão Inovação e Conhecimento (2002), Agência para a Sociedade do Conhecimento, I. P. (2005), na tutela da PCM até 2006
- Presidida pelo Dr. Diogo Vasconcelos (1968 – 2011)
- Diversos Projetos de Inovação, alguns com uma forte componente de segurança (voto eletrónico, comércio eletrónico, primórdios do Cartão de Cidadão, assinatura eletrónica, etc…)
- Identificação da necessidade de criar um projeto autónomo e transversal para a segurança da informação (2004)
- Convite a entidades com interesses na matéria:

- **Estrutura Nacional de Segurança da Informação – ENSI** (2005, XVI Gov. Constitucional)

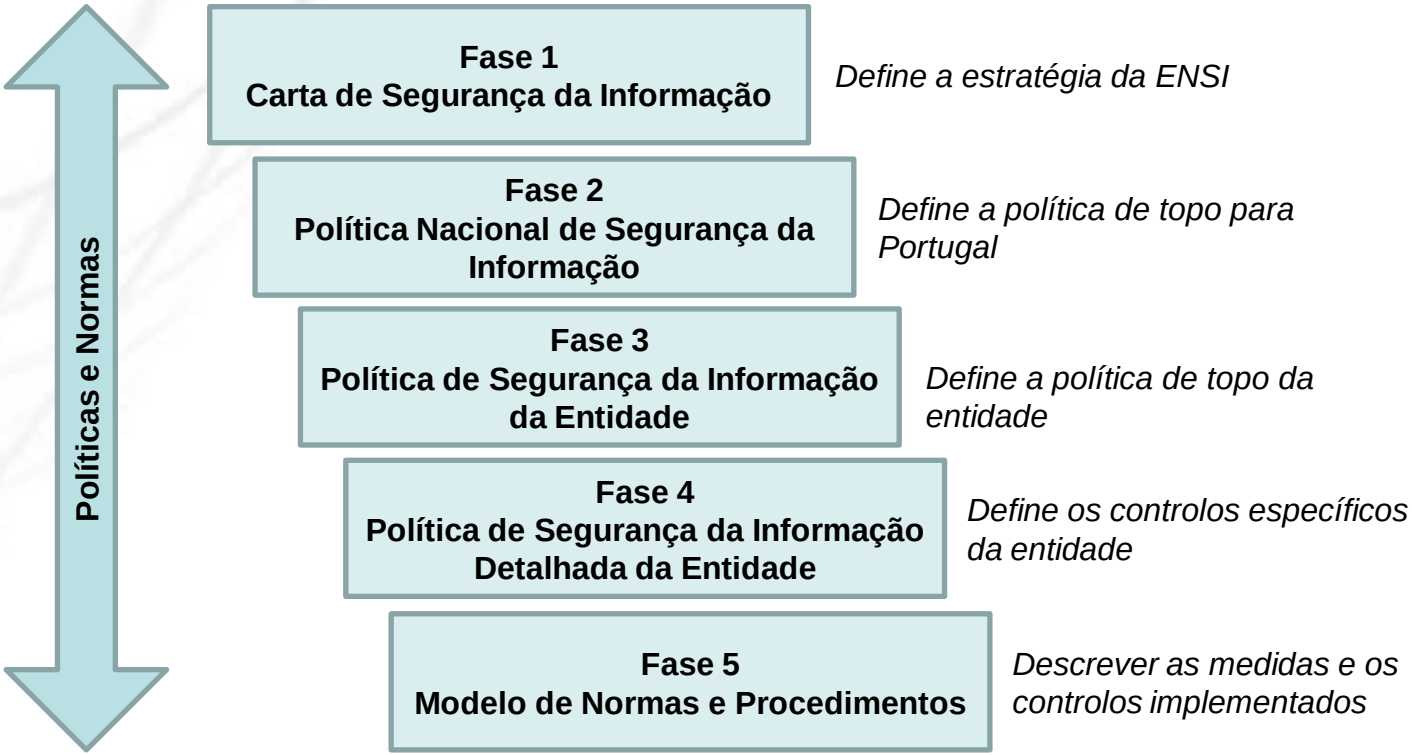
Levantamento e Análise da Situação

- Identificadas cerca de 30 entidades relevantes em Portugal
- Foram efetuadas mais de 20 entrevistas
- Identificadas cerca de 32 entidades internacionais relevantes
- Avaliados 6 Planos Nacionais de Segurança Digital de outras Nações



Estrutura Nacional de Segurança da Informação

Plano de Ação (8 fases)



Estrutura Nacional de Segurança da Informação

Plano de Ação (8 fases) *(continuação)*

Fase 6
Consciencialização

Criar uma cultura de segurança entre os cidadãos, trabalhadores e gestores

Fase 7
PKI Nacional

Estabelecer uma PKI Nacional

Fase 8
CSIRT

Formalizar responsabilidade e hierarquias para resposta a incidentes de segurança de computadores (CSIRT)

Estratégia de Comunicação

Carta de Segurança da Informação

- **Missão:** O Governo Português estabelece a Estrutura Nacional de Segurança da Informação (ENSI) em benefício da Sociedade da Informação nacional. A ENSI instrui o sector público (obrigatório) e guia o sector privado (recomendado), através da definição de objetivos de segurança e estabelece uma política de topo para a Segurança da Informação. A ENSI tem como objetivo facilitar a coordenação de todos os esforços de Segurança da Informação, dinamizando a implementação de uma cultura nacional de segurança e minimizando a duplicação de recursos e competências.
- **Objetivos:**
  - **Objetivo 1:** *Proteger as infraestruturas críticas portuguesas através de medidas eficazes e coordenadas de segurança da informação*
  - **Objetivo 2:** *Assegurar de forma segura a interoperabilidade da infraestrutura da informação portuguesa, através da aplicação consistente da segurança da informação nos sectores público e privado.*
  - **Objetivo 3:** *Melhorar a cultura da segurança da informação nas organizações públicas e privadas e acelerar a sua implementação*
  - **Objetivo 4:** *Promover a pesquisa e melhorar as capacidades de análise de ameaças e vulnerabilidades relativamente à Segurança da Informação.*
  - **Objetivo 5:** Desenvolver e executar uma infraestrutura eletrónica nacional de autenticação que abranja os sectores público e privado.
  - **Objetivo 6:** Proteger a privacidade e os interesses pessoais do consumidor na Sociedade da Informação.
  - **Objetivo 7:** Aumentar a consciência pública relacionada com os requisitos da segurança da informação em Portugal.

Política Nacional de Segurança da Informação

- **Objetivos:**
  - **Objectivo 1:** *Ser parte integrante dos objectivos da Administração Pública e servir de orientação ao sector privado.*
  - **Objectivo 2:** *Proteger os interesses do estado e seus cidadãos, as entidades públicas e privadas e seus clientes e os parceiros e seus empregados.*
  - **Objectivo 3:** *Assegurar que todos os requisitos legais e da Indústria são cumpridos e que existe o registo de evidências, para efeitos de auditoria, de todos os processos TIC relevantes em cada entidade do sector público ou privado.*
  - **Objectivo 4:** *Assegurar que a Política de Segurança da Informação da Entidade é implementada por uma equipa de Segurança da Informação, de acordo com as normas de Segurança da Informação mandatárias. As entidades do sector privado são incentivadas a proceder da mesma forma.*
  - **Objectivo 5:** *Consciencializar para a segurança todos os funcionários públicos e empregados de empresas do sector privado que fornecem serviços de infra-estrutura crítica.*
  - **Objectivo 6:** *Assegurar a protecção de dados e recursos das TIC através de iniciativas adequadas a tomar por cada membro da Sociedade da Informação.*
  - **Objectivo 7:** *Assegurar um elevado nível de Segurança da Informação durante todo o ciclo de vida dos sistemas de informação.*
  - **Objectivo 8:** *Garantir a continuidade do negócio.*
  - **Objectivo 9:** *Honrar a confiança de todos os membros da Sociedade da Informação.*

Política Nacional de Segurança da Informação

- **Responsabilidades:**
  - **Nacional –** Comité ENSI
  - **Ministerial –** Estrutura de Gestão por Tutela
  - **Departamental –** Responsáveis ou equipas de INFOSEC
  - **Sociedade da Informação –** Sensibilização a todos os níveis e responsabilização individual

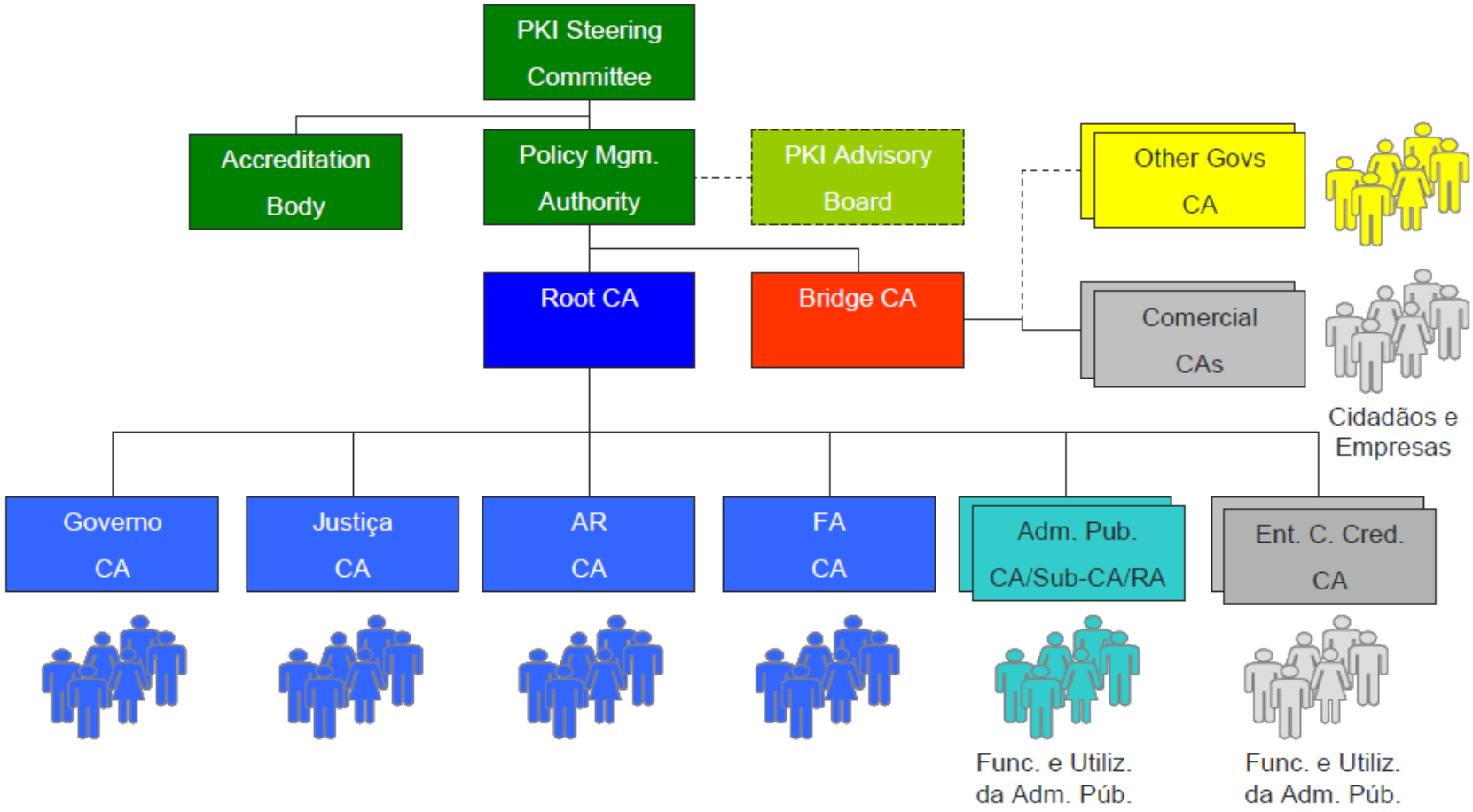
Consciencialização

- **Segurança da Informação para o Cidadão**
  - Vírus (malware); Senhas (passwords); Utilização da Internet; Correio Electrónico; Privacidade.

- **Segurança da Informação no Trabalho**
  - Riscos Potenciais; Confidencialidade de Dados; Classificação de Dados; Armazenamento de Dados; Transmissão de Dados; Destruição de Dados; Cópia de Segurança de Dados; Fidelidade dos Dados; Vírus; Boas/Más Práticas.

- **Segurança da Informação para o Gestor**
  - Segurança da Informação
  - Gestão de Risco (Identificação de Activos; Ameaças; Vulnerabilidades; Controlos de Segurança; Análise de Risco)

PKI Nacional - Recomendações



Resposta a Incidentes - CSIRT

- **Não foi elaborado qualquer documento especifico**
- **Várias referências em vários documentos:**
  - **Carta de Segurança da Informação – Objectivo 4, criação de um CSIRT central.**
  - **Política de Segurança da Informação – Serviços de Segurança da Informação:**

    "O comité ENSI estabelecerá uma equipa nacional de resposta a incidentes de Segurança da Informação, sem fins lucrativos para a Sociedade da Informação. Esta será uma fonte de informação sobre as últimas vulnerabilidades que afectam as TIC e sobre as estratégias relevantes de resposta e recuperação. Esta facilitará o acesso a um serviço de alerta de Segurança da Informação, no sentido de recolher e analisar relatórios acerca de incidentes de Segurança da Informação e melhor informar o público Português."
  - **Análise da Segurança da Informação – Fase 8:**
    - Criação de um CSIRT Nacional
    - Apoio na resolução de incidentes; Disseminação de alertas, recomendações e boas práticas; Formação e qualificação; Colaboração com fabricantes; Coordenação e representação nacional e internacional.

REVISÃO DA ENSI

- **Reavaliação da situação, incluindo infraestruturas críticas**
- **Revisão de conteúdos face à realidade atual**
- **Introdução de novos capítulos**
  - **Política de Segurança da Informação para o Prestadores de Serviços TIC**
  - **Governance da Estrutura Nacional de Cibersegurança**
  - **Governance das Soluções Criptográficas Nacionais**

Centro Nacional de Cibersegurança

- **RCM n.º 42/2012 – Criação da Comissão Instaladora do Centro Nacional de Cibersegurança**
  - **9 Entidades**
  - **4 Personalidades de reconhecido mérito**
  - **Equipa Multidisciplinar**
  - **Presidida pela Autoridade Nacional de Segurança**
- **Apresentação do Relatório Final em Junho de 2012**
  - **Implementação faseada**
  - **Entre 2013 – 2015**
  - **Dependência Direta do PM**
  - **Autoridade sobre entidades do Estado e progressivamente extensívela a infraestruturas críticas**
  - **Capacidade operacional e de resposta**
  - **Competências de autoridade técnica e de doutrina**
  - **Interlocutor com entidades estrangeiras congéneres (Nações, NATO, EU, …)**

Outras Ações da Medida 04

- **Sistema de Certificação Eletrónica do Estado**
  - **Implementação 2013 e 2014**
  - **Impacto da Medida 12 do GPTIC**

- **Criptografia Nacional**
  - **Solução criptográfica forte para informação e comunicações IP**
  - **Solução criptográfica para comunicações móveis**
  - **Desenvolvimentos com a estrutura de I&D nacional (universidades, institutos e empresas)**

- **Quadro Legal para a Segurança das Matérias Classificadas**
  - **Projeto de Lei submetido à AR**
  - **Enquadramento com o quadro legal de "Segredo de Estado"**

Missão do CEGER

Prestador de serviços na área das
tecnologias de informação e comunicação…

… a um cliente muito especial e de elevada sensibilidade…

… e que, por sinal, também é o seu "patrão".

Visão Integrada e Multifacetada

- Garantir [illegible]utilizadores autorizados e com nec[illegible]
- Assegura[illegible]terada ou manipulada de forma ilíc[illegible]
- Proporci[illegible]onde e quando esta for necessár[illegible]
- Verificar [illegible]
- Manter c[illegible]ocessos e ações de elaboraç[illegible]
  informaçã[illegible]

CONFIDENCIALIDADE

INTEGRIDADE

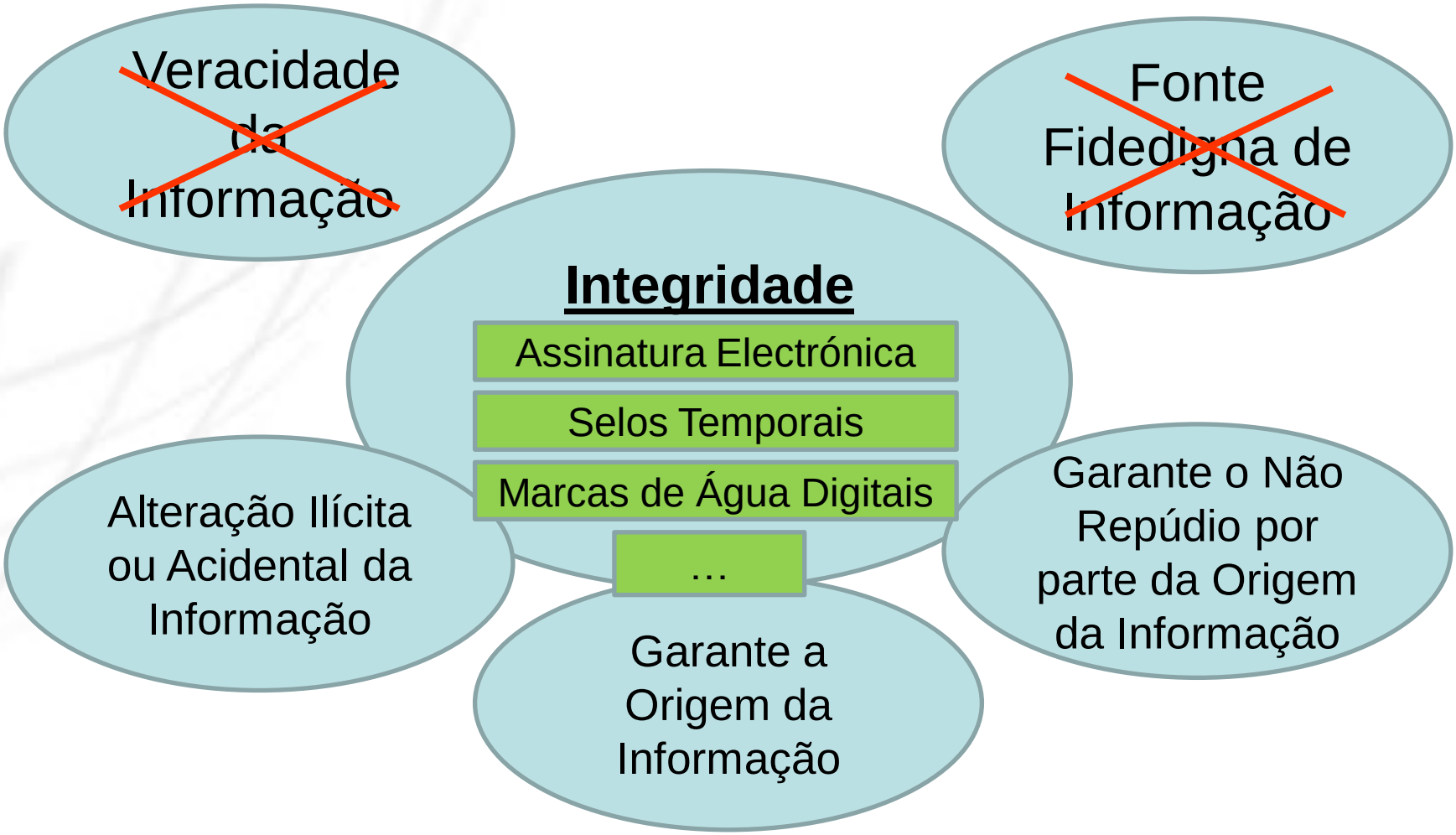
DISPONIBILIDADE

ACCOUNTABILITY
(Responsabilidade)

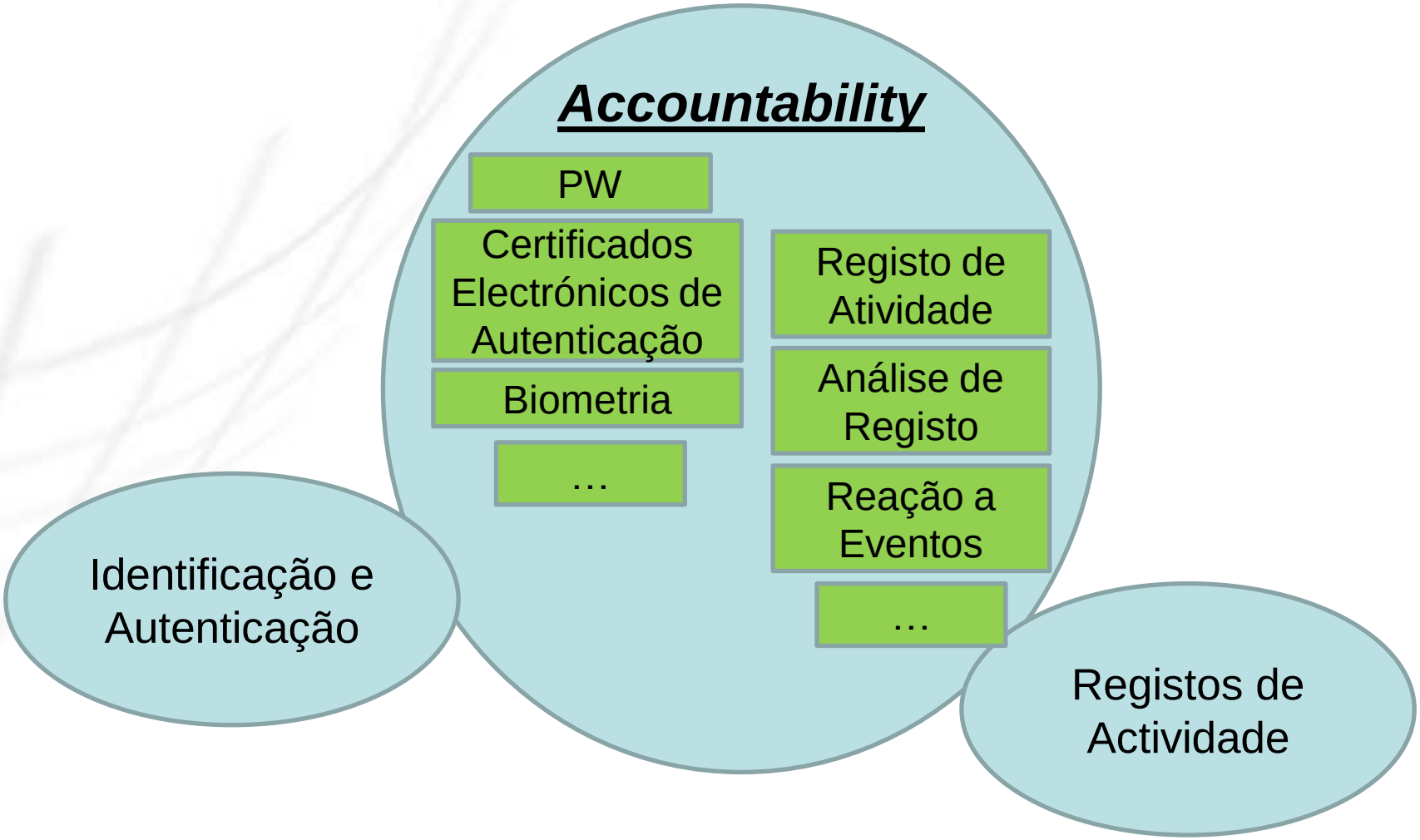
Identidade e Autenticação

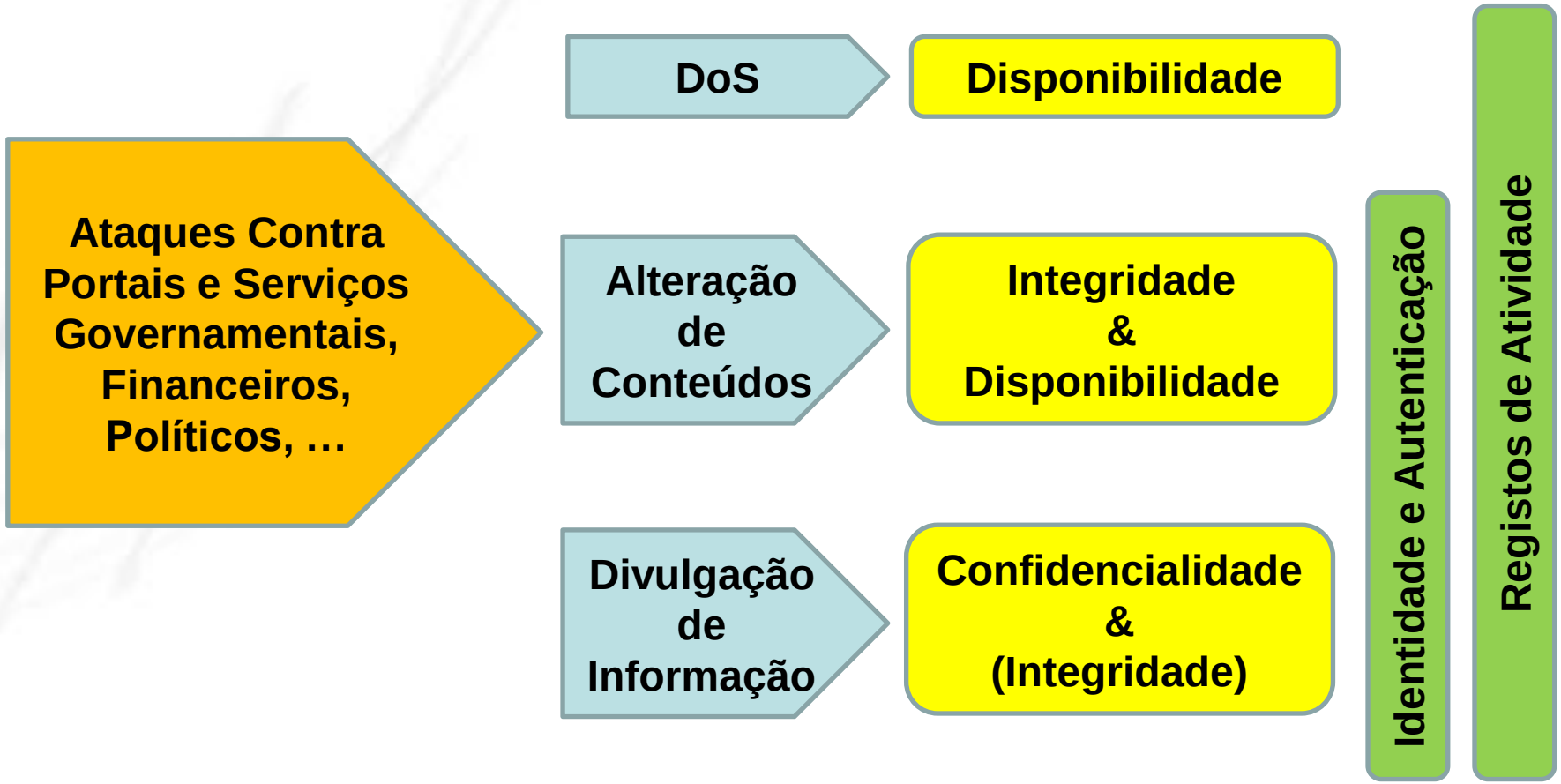
Registos


Matérias Classificadas
Privacidade no Local de Trabalho
Confidencialidade
Cifras
Controlos de Acesso
Gestão de Direitos / Utilizadores
Gestão de Políticas
...
Matérias Executivas Sensíveis
Matérias Técnicas Sensíveis
Matérias Políticas Sensíveis

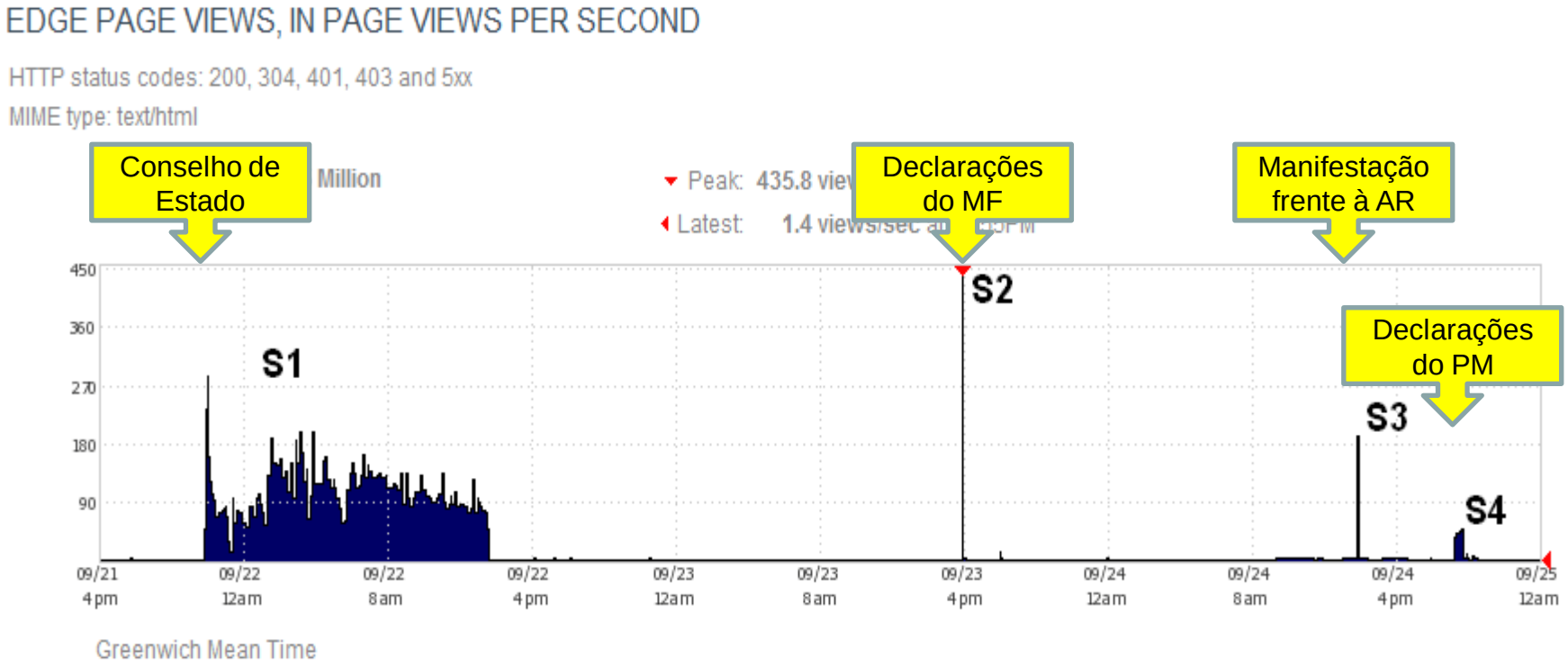

Veracidade da Informação
Fonte Fidedigna de Informação
Integridade
Assinatura Electrónica
Selos Temporais
Marcas de Água Digitais
…
Alteração Ilícita ou Acidental da Informação
Garante o Não Repúdio por parte da Origem da Informação
Garante a Origem da Informação


Dever da Publicidade e Transparência na AP
Direito de Acesso à Informação
Disponibilidade
Redundância e Resiliência
Mobilidade
Interoperabilidade
Capacidade de Resposta
…
A Quem Necessita
No Formato Adequado
Onde for Necessária
Quando for Necessária


Accountability
PW
Certificados Electrónicos de Autenticação
Biometria
…
Registo de Atividade
Análise de Registo
Reação a Eventos
…
Identificação e Autenticação
Registos de Actividade


Ataques Contra Portais e Serviços Governamentais, Financeiros, Políticos, …
DoS
Disponibilidade
Alteração de Conteúdos
Integridade & Disponibilidade
Divulgação de Informação
Confidencialidade & (Integridade)
Identidade e Autenticação
Registos de Atividade

Situações identificadas entre os dias 21 e 24 de Setembro, 2012



S1 – Sexta (22 SET) a Sábado (23 SET), das 23h às 15h
S2 – Domingo (23 SET), às 17h
S3 – Segunda (24 SET), às 15h
S4 – Segunda (24 SET), das 20h15 às 20h45

Nota: As horas são aproximadas.

Conclusões (GPTIC)

- Portugal em 2005 era vanguarda na Europa e na NATO para a criação de uma ENSI, em 2012 é um dos países mais atrasados nesta matéria
- A abrangência deverá extravasar o Estado, englobando toda a sociedade da informação e Infraestruturas Críticas
- A ENSI de 2004/2005, após 7 anos, continua a ser bastante atual requerendo uma revisão para a adaptar aos novos cenários de ameaça e aos novos conceitos de segurança
- Centro Nacional de Cibersegurança (CNCSeg), não é uma opção, é uma obrigação de Portugal perante os seus pares e uma necessidade de sobrevivência
- Modelo do CNCSeg, …

Conclusões (CEGER)

- Adequação ao cliente e à área de negócio;
- Visão Integrada e Multifacetada (Confidencialidade, Integridade, Disponibilidade e *Accountability*);
- Delimitação do âmbito de aplicação de cada factor;
- Capacidade de Gestão e Reação;
- Maleabilidade, Inovação e Aprendizagem
- Segurança da Informação é:
  - 30% Tecnologia
  - 30% Política/Processos e Pedagogia
  - 30% Bom Senso
  - 10% Marketing

GOVERNO DE PORTUGAL
PRESIDÊNCIA DO CONSELHO DE MINISTROS

Obrigado!

CEGER
CENTRO DE GESTÃO DA REDE INFORMÁTICA DO GOVERNO
CMG Eng. Manuel Honorato
Rua Almeida Brandão, 7
1200-602 Lisboa
PORTUGAL
Telefone: +351 21 3923400
Fax: +351 21 3923499
E-mail: manuel.honorato@ceger.gov.pt
Homepage: http://www.ceger.gov.pt