INF 108

Segurança da Informação

Computação em Nuvem

Prof. João Henrique Kleinschmidt

Introdução

- Centralização do processamento
  - Surgimento da Teleinformática – Década de 60
- Execução de programas localmente
  - Computadores Pessoais – Década de 80
- Migração de programas e dados para a Internet
  - Computação em Nuvem – Atual

História

- Mainframes (≈ 1950-80)
- Micro-computadores (80's)
- Cliente-Servidor (80)
- WWW (≈ 1992)
- Telefonia Móvel (≈ 1995)
- Grid Computing (≈ 1995)
- VMware e Xen (≈ 1999)
- SalesForce.com (≈ 1999)
- SUN's Thin Client Computing (≈ 1999)
- Representational State Transfer (REST) - *Roy Fielding's PhD* (2000)
- Banda Larga (>2000)
- Writley/Google Apps/Zoho – Office prod. Apps (≈ 2005)
- Amazon WS (≈ 2005)
- Apache's Hadoop (≈ 2005)
- ...

Duas Tecnologias

- **Virtualização:**

  *Habilidade de executar múltiplos sistemas operacionais em um único sistema de hardware e compartilhar os recursos de hardware**

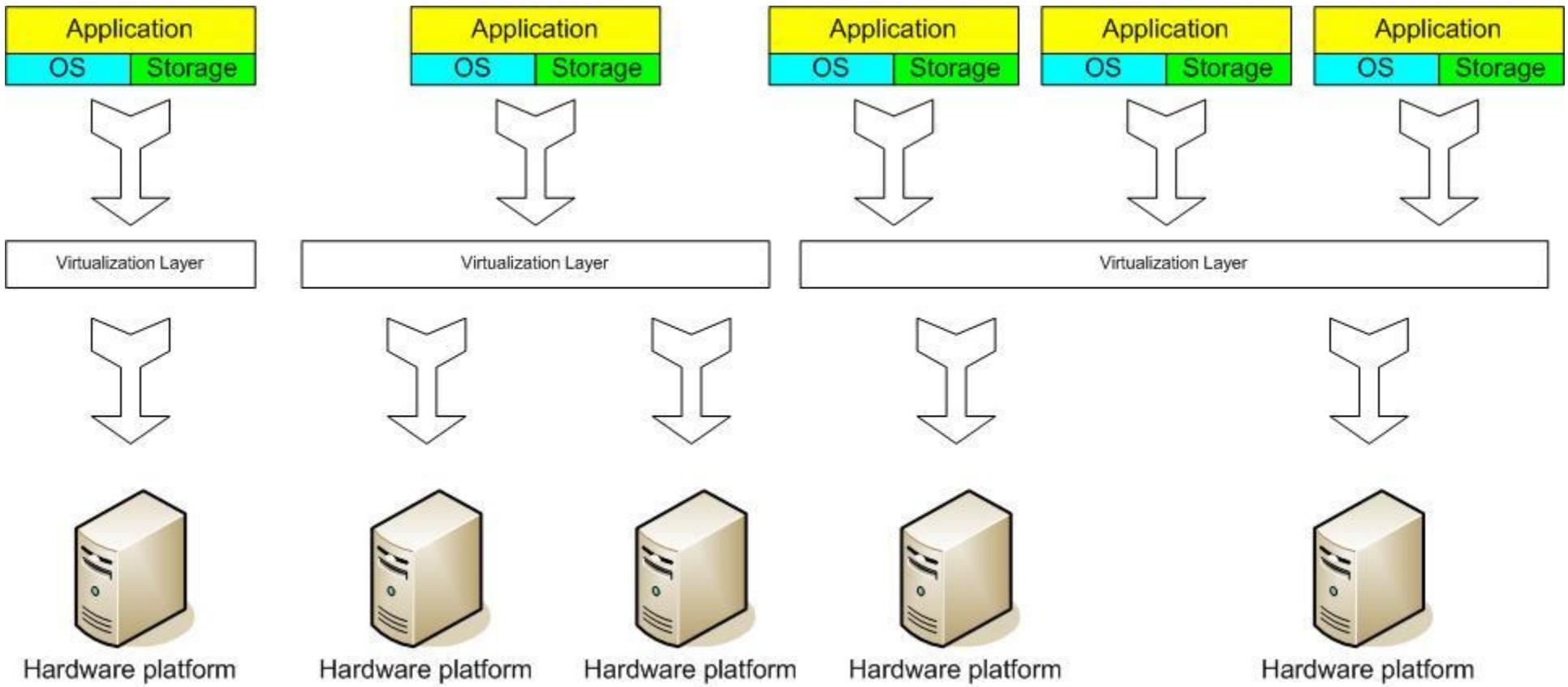
- **Computação em Nuvem:**

  *Provisão de serviços por demanda. The provisioning of services in a timely (near on instant), on-demand manner, to allow the scaling up and down of resources"***

* VMware white paper, *Virtualization Overview*

** Alan Williamson, quoted in *Cloud BootCamp March 2009*

Conceito de Servidor Virtual



Camada do monitor de máquina virtual (VMM) entre *SO* convidado e hardware

Conceito de Servidor Virtual

- Vantagens
  - Alocação de recursos
  - Alta redundância
  - Alta disponibilidade
  - Rápida implantação de servidores
  - Reconfigurável enquanto servidores estão executando
  - Otimização de recursos físicos
- Desvantagens
  - Mais difícil de projetar
  - Eventualmente mais caros

Computação em nuvem leva virtualização para o próximo passo!

- **Você não precisa ter o hardware**
- "Aluga" de acordo com a necessidade

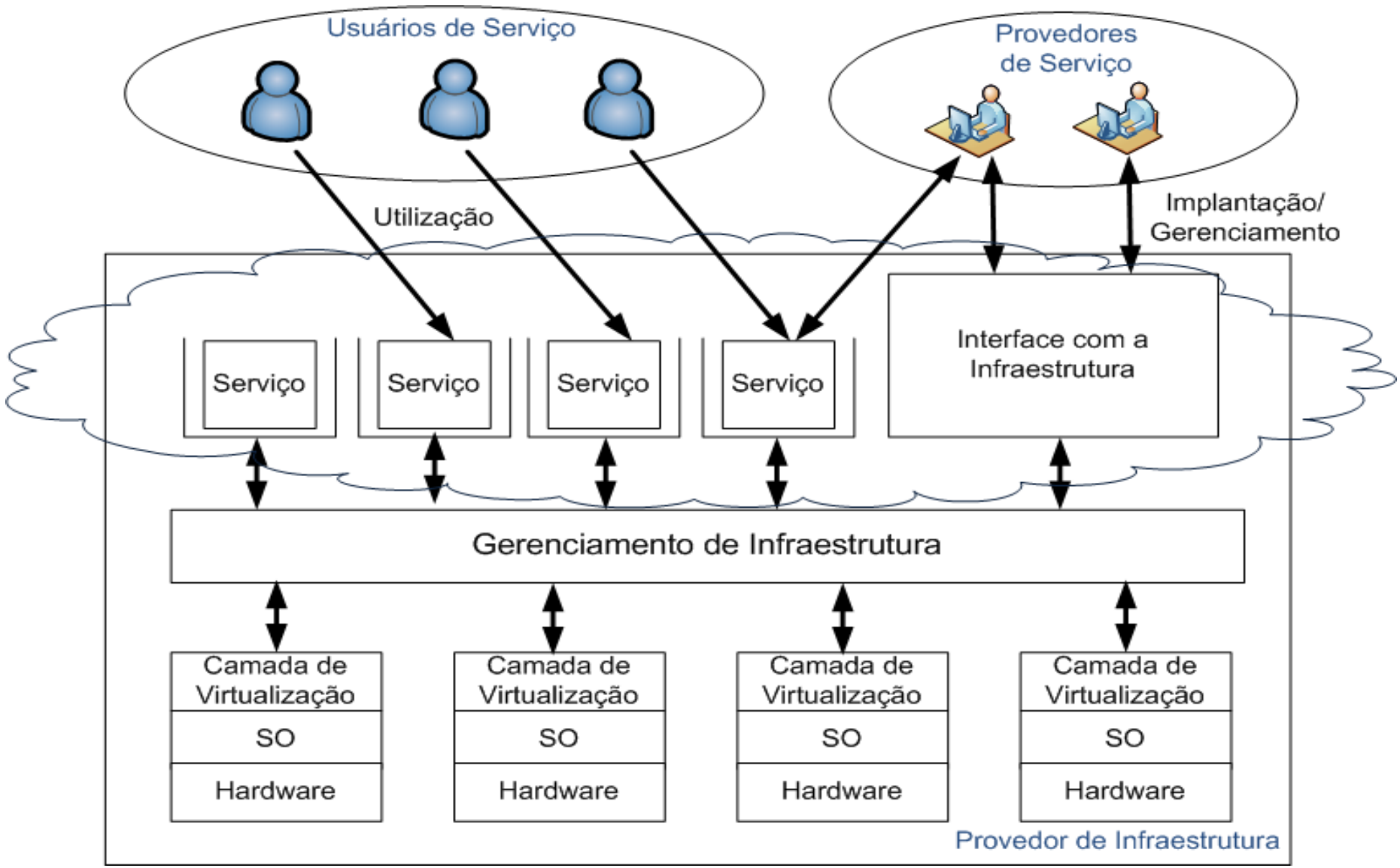
Definição

" *A Nuvem é um grande reservatório de recursos virtualizados facilmente utilizáveis e acessíveis (como hardware, plataformas de desenvolvimento e/ou serviços). Esses recursos podem ser dinamicamente reconfigurados para ajustar a carga (escala) variável do sistema, permitindo também um uso ótimo dos recursos. Esse reservatório de recursos é geralmente explorado por um modelo pay-per-use (pagar para usar) no qual as garantias são oferecidas por um Provedor de Infraestrutura por meio de SLAs (Service Level Agreement - Acordo de Nível de Serviço)* "

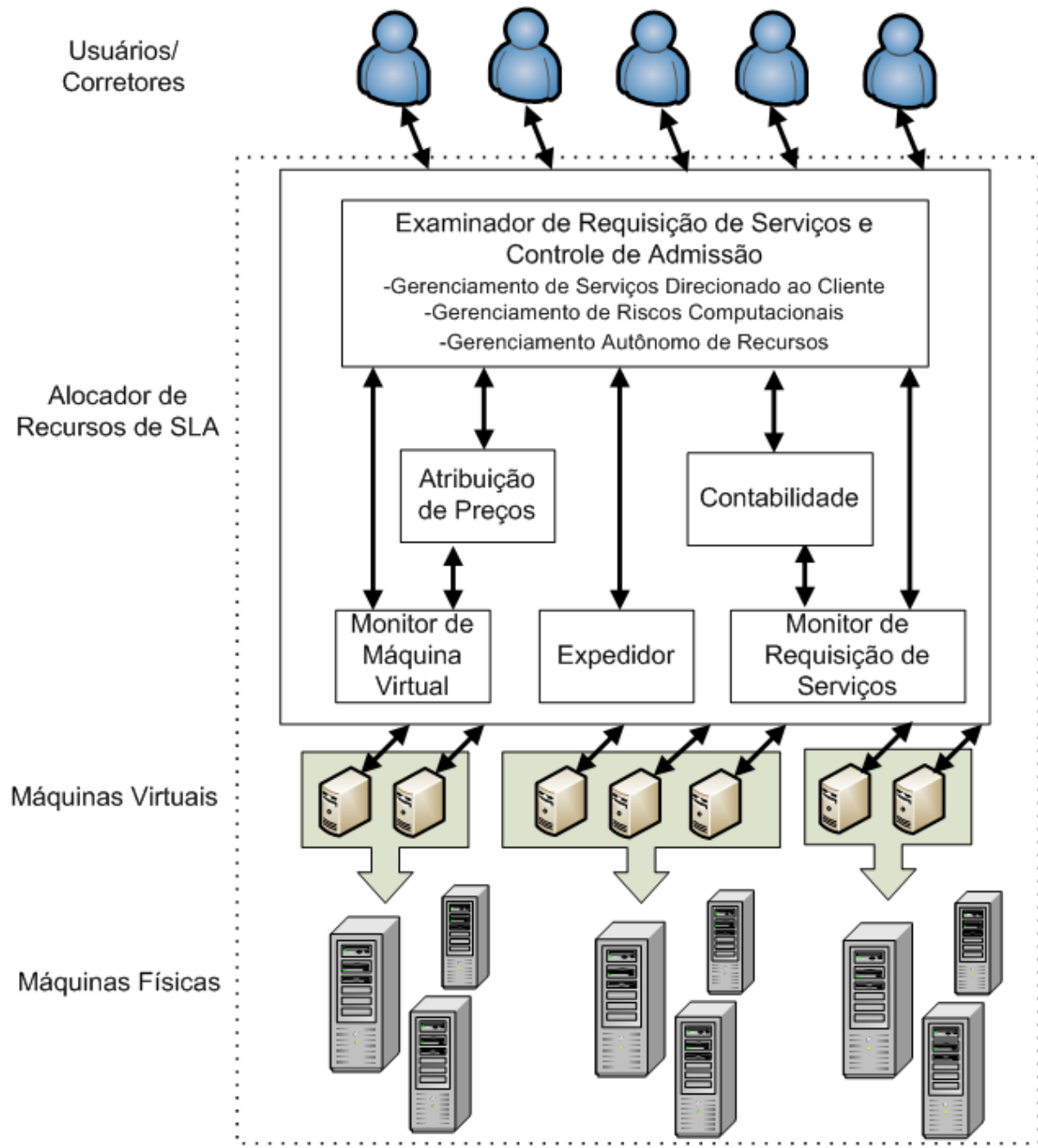
Retirado de:

Vaquero, L.M. and Rodero-Merino, L. and Caceres, J. and Lindner, M. "A break in the clouds: towards a cloud definition" em ACM SIGCOMM Computer Communication Review, 2008

Computação em Nuvem



Arquitetura



Características

Características Comuns:

- Escala Massiva
- Computação Resiliente
- Homogeneidade
- Distribuição Geográfica
- Virtualização
- Orientada a Serviços
- Software Baixo Custo
- Segurança Avançada

Características essenciais:

- Serviços por Demanda
- Acesso Rede Banda Larga
- Elasticidade
- Varredura de Recursos
- Medição de Serviços

Tipos de Cenário

- **Infraestrutura como Serviço (IaaS):**
  - Sistema Operacional completo
- **Plataforma como Serviço (PaaS):**
  - Ambiente de desenvolvimento
- ***Software* como Serviço (SaaS):**
  - Editores de texto

Software as a Service (SaaS)

- Aplicações completas ou conjuntos de aplicações disponíveis pela Web
- Varios modos de cobrança por uso
- Customização de aplicações
- Modos de uso offline

Exemplos:

- Salesforce.com
- NetSuite
- Ariba - spend mngt sw
- Zoho App Suite
- RightNow
- Google Apps
- SAP Business ByDesign
- ~FaceBook

Platform as a Service (PaaS)

Platformas internet para desenvolver, testar, implantar e executar aplicações próprias, com:

- IDE
- Linguagem padrão ou propritária
- Abstrações de alto nível

Exemplos:

- Force.com
- Google App Engine
- Bungee
- LongJump
- Intuit Quickbase
- Coghead (SAP)
- Etelos

Infrastructure as a Service (IaaS)

Hardware virtual disponibilizado como serviço

- VMs / poder de processamento
- Storage
- Network (f/w, nlbs)

Infra-estruturas de Software virtual

- Banco de Dados
- Messaging (MOM)
- Processamento

Exemplos:

- Amazon Web Services (AWS): EC2, S3, SimpleDB, SQS, MapReduce
- GoGrid
- Flexiscale
- Google App Engine, Gdata
- Rackspace / Mosso
- Cloudera
- Hadoop
- Eucapyptus
- Nimbus

Modelos de Desenvolvimento

Nuvem pública

- As nuvens públicas são aquelas que são executadas por terceiros. As aplicações de diversos usuários ficam misturadas nos sistemas de armazenamento. Um dos benefícios das nuvens públicas é que elas podem ser muito maiores do que uma nuvem privada, por exemplo, já que elas permitem uma maior escalabilidade dos recursos. Essa característica evita a compra de equipamentos adicionais para resolver alguma necessidade temporária, deslocando os riscos de infraestrutura para os prestadores de infraestrutura da nuvem.

Nuvem privada

As nuvens privadas são aquelas construídas exclusivamente para um único usuário (uma empresa, por exemplo). Diferentemente de um *data center* privado virtual, a infraestrutura utilizada pertence ao usuário, e, portanto, ele possui total controle sobre como as aplicações são implementadas na nuvem. Uma nuvem privada é, em geral, construída sobre um *data center* privado.

Nuvem híbrida

As nuvens híbridas combinam os modelos das nuvens públicas e privadas. Elas permitem que uma nuvem privada possa ter seus recursos ampliados a partir de uma reserva de recursos em uma nuvem pública. Essa característica possui a vantagem de manter os níveis de serviço mesmo que haja flutuações rápidas na necessidade dos recursos.

Nuvem comunitária

- Uma nuvem comunitária é formada quando várias organizações com requisitos similares compartilham uma infraestrutura.

Modelos

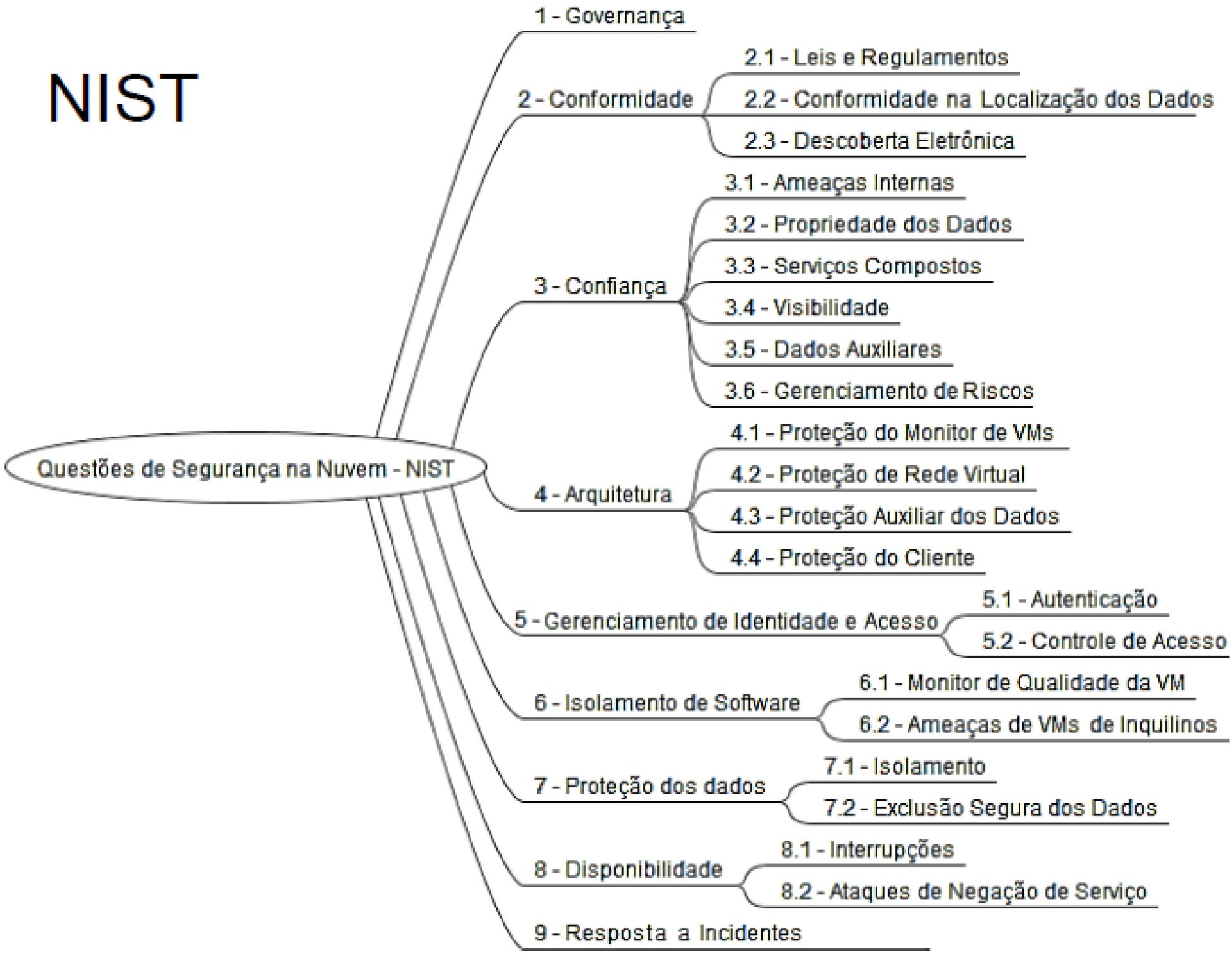
Modelo Implantação	Gerência	Propriedade	Localização	Segurança
Pública	Terceiros	Terceiros	Externa ou Interna	Baixa
Privada	Própria	Própria ou Terceiros	Interna	Alta
Comunitária	Própria ou Terceiros	Própria ou Terceiros	Externa ou Interna	Média
Híbrida	Própria ou Terceiros	Própria ou Terceiros	Externa ou Interna	Média

Guias de segurança para computação em nuvem

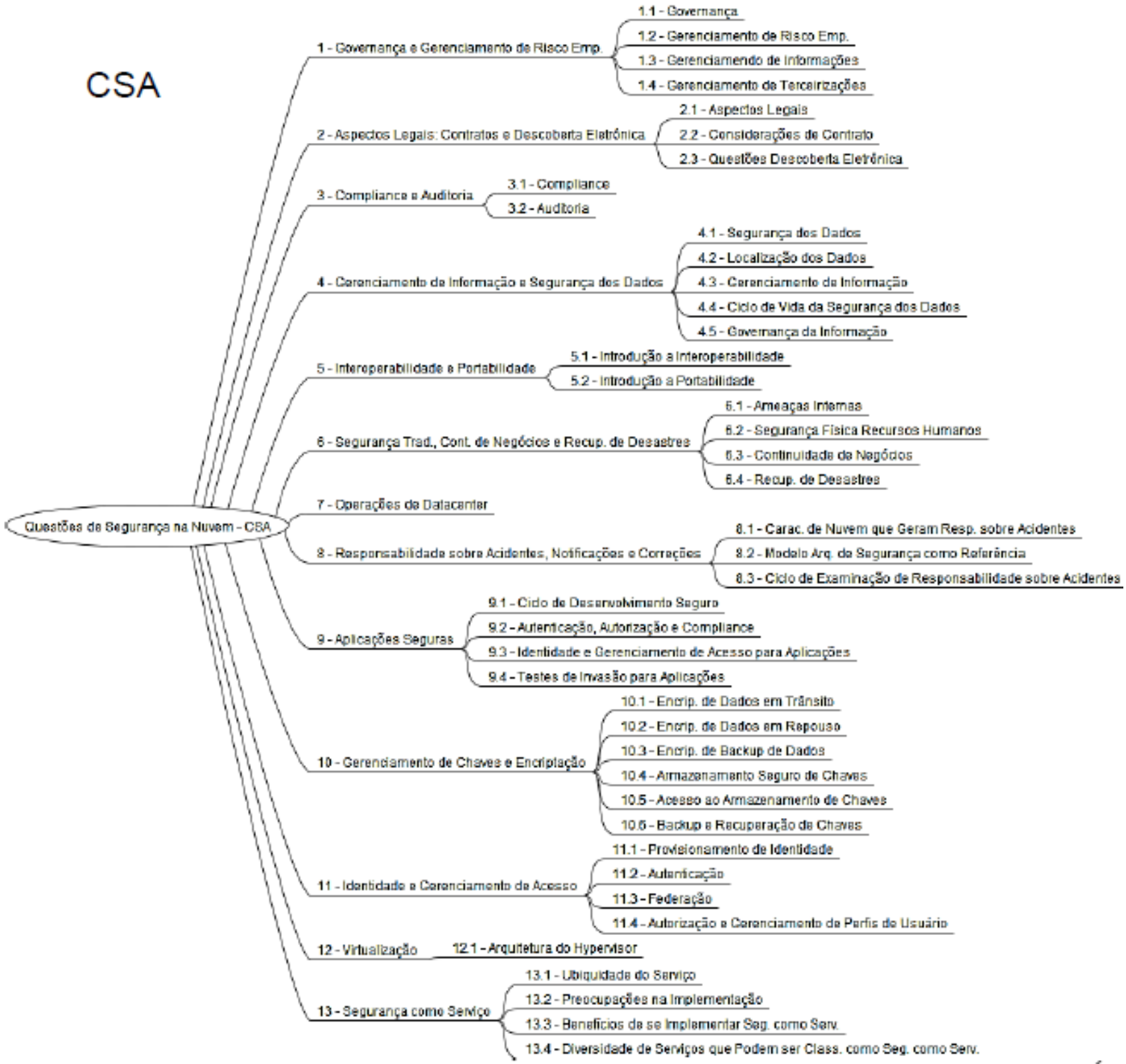
- A computação em nuvem já possui materiais de referência que cobrem os aspectos gerais de segurança, providos na forma de documentos, guias e padrões.

- Principais guias foram elaborados por:
- CSA – Cloud Security Alliance
  - https://cloudsecurityalliance.org/
- ENISA - European Network and Information Security Agency
  - https://www.enisa.europa.eu/
- NIST - National Institute of Standards and Technology
  - http://www.nist.gov/itl/cloud/

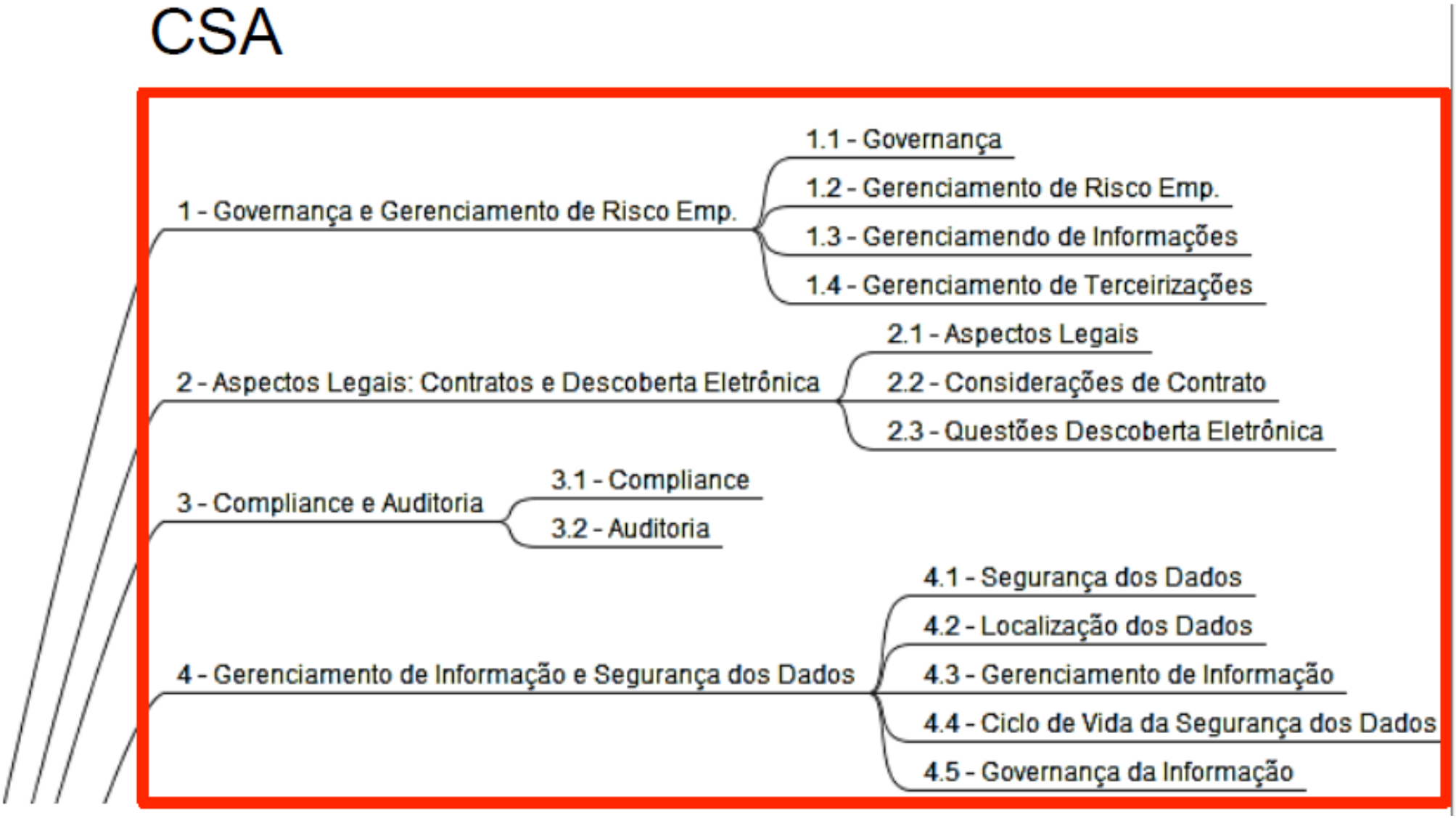
NIST


Questões de Segurança na Nuvem - NIST
1 - Governança
2 - Conformidade
2.1 - Leis e Regulamentos
2.2 - Conformidade na Localização dos Dados
2.3 - Descoberta Eletrônica
3 - Confiança
3.1 - Ameaças Internas
3.2 - Propriedade dos Dados
3.3 - Serviços Compostos
3.4 - Visibilidade
3.5 - Dados Auxiliares
3.6 - Gerenciamento de Riscos
4 - Arquitetura
4.1 - Proteção do Monitor de VMs
4.2 - Proteção de Rede Virtual
4.3 - Proteção Auxiliar dos Dados
4.4 - Proteção do Cliente
5 - Gerenciamento de Identidade e Acesso
5.1 - Autenticação
5.2 - Controle de Acesso
6 - Isolamento de Software
6.1 - Monitor de Qualidade da VM
6.2 - Ameaças de VMs de Inquilinos
7 - Proteção dos dados
7.1 - Isolamento
7.2 - Exclusão Segura dos Dados
8 - Disponibilidade
8.1 - Interrupções
8.2 - Ataques de Negação de Serviço
9 - Resposta a Incidentes

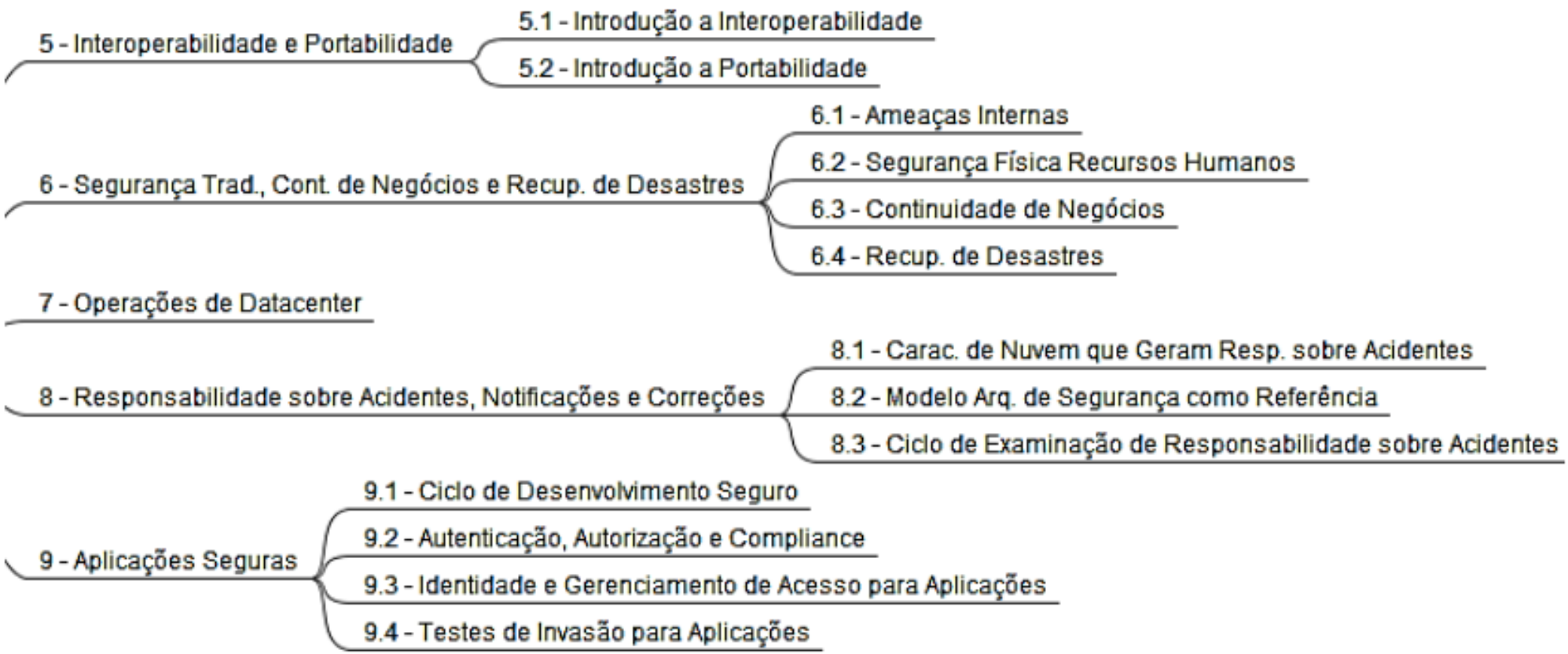
CSA


Questões de Segurança na Nuvem - CSA
1 - Governança e Gerenciamento de Risco Emp.
1.1 - Governança
1.2 - Gerenciamento de Risco Emp.
1.3 - Gerenciamendo de Informações
1.4 - Gerenciamento de Tercerizações
2 - Aspectos Legais: Contratos e Descoberta Eletrônica
2.1 - Aspectos Legais
2.2 - Considerações de Contrato
2.3 - Questões Descoberta Eletrônica
3 - Compliance e Auditoria
3.1 - Compliance
3.2 - Auditoria
4 - Gerenciamento da Informação e Segurança dos Dados
4.1 - Segurança dos Dados
4.2 - Localização dos Dados
4.3 - Gerenciamento da Informação
4.4 - Ciclo de Vida da Segurança dos Dados
4.5 - Governança da Informação
5 - Interoperabilidade e Portabilidade
5.1 - Introdução a Interoperabilidade
5.2 - Introdução a Portabilidade
6 - Segurança Trad., Cont. de Negócios e Recup. de Desastres
6.1 - Ameaças Internas
6.2 - Segurança Física Recursos Humanos
6.3 - Continuidade de Negócios
6.4 - Recup. de Desastres
7 - Operações do Datacenter
8 - Responsabilidade sobre Acidentes, Notificações e Correções
8.1 - Carac. de Nuvem que Geram Resp. sobre Acidentes
8.2 - Modelo Arq. de Segurança como Referência
8.3 - Ciclo de Examinação de Responsabilidade sobre Acidentes
9 - Aplicações Seguras
9.1 - Ciclo de Desenvolvimento Seguro
9.2 - Autenticação, Autorização e Compliance
9.3 - Identidade e Gerenciamento de Acesso para Aplicações
9.4 - Testes de Invasão para Aplicações
10 - Gerenciamento de Chaves e Encriptação
10.1 - Encrip. de Dados em Trânsito
10.2 - Encrip. de Dados em Repouso
10.3 - Encrip. de Backup de Dados
10.4 - Armazenamento Seguro de Chaves
10.5 - Acesso ao Armazenamento de Chaves
10.6 - Backup e Recuperação de Chaves
11 - Identidade e Gerenciamento de Acesso
11.1 - Provisionamento de Identidade
11.2 - Autenticação
11.3 - Federação
11.4 - Autorização e Gerenciamento de Perfis de Usuário
12 - Virtualização
12.1 - Arquitetura do Hypervisor
13 - Segurança como Serviço
13.1 - Ubiquidade do Serviço
13.2 - Preocupações na Implementação
13.3 - Benefícios de se Implementar Seg. como Serv.
13.4 - Diversidade de Serviços que Podem ser Class. como Seg. como Serv.

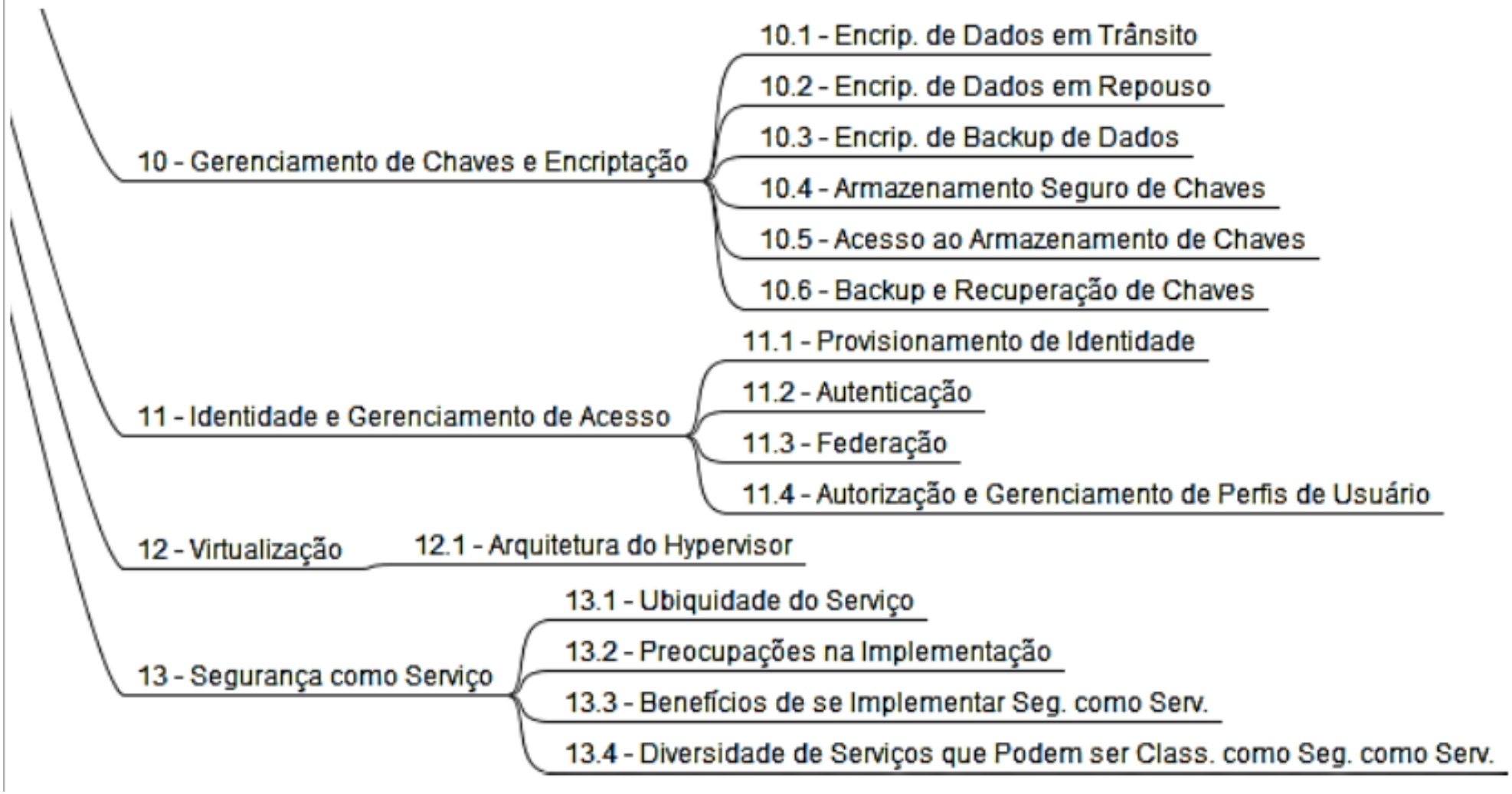
CSA


1 - Governança e Gerenciamento de Risco Emp.
1.1 - Governança
1.2 - Gerenciamento de Risco Emp.
1.3 - Gerenciamendo de Informações
1.4 - Gerenciamento de Terceirizações
2 - Aspectos Legais: Contratos e Descoberta Eletrônica
2.1 - Aspectos Legais
2.2 - Considerações de Contrato
2.3 - Questões Descoberta Eletrônica
3 - Compliance e Auditoria
3.1 - Compliance
3.2 - Auditoria
4 - Gerenciamento de Informação e Segurança dos Dados
4.1 - Segurança dos Dados
4.2 - Localização dos Dados
4.3 - Gerenciamento de Informação
4.4 - Ciclo de Vida da Segurança dos Dados
4.5 - Governança da Informação

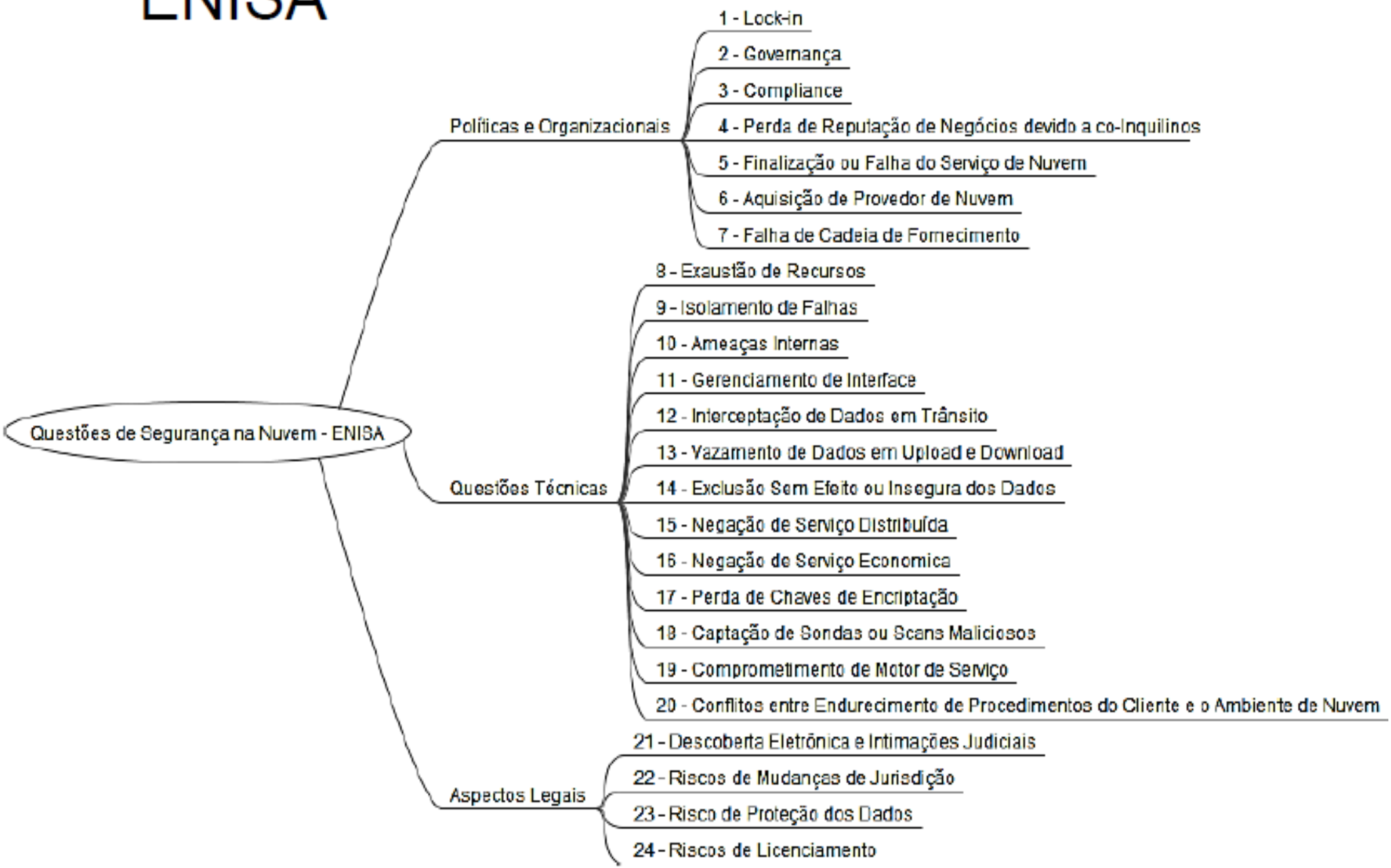
CSA


5 - Interoperabilidade e Portabilidade
5.1 - Introdução a Interoperabilidade
5.2 - Introdução a Portabilidade
6 - Segurança Trad., Cont. de Negócios e Recup. de Desastres
6.1 - Ameaças Internas
6.2 - Segurança Física Recursos Humanos
6.3 - Continuidade de Negócios
6.4 - Recup. de Desastres
7 - Operações de Datacenter
8 - Responsabilidade sobre Acidentes, Notificações e Correções
8.1 - Carac. de Nuvem que Geram Resp. sobre Acidentes
8.2 - Modelo Arq. de Segurança como Referência
8.3 - Ciclo de Examinação de Responsabilidade sobre Acidentes
9 - Aplicações Seguras
9.1 - Ciclo de Desenvolvimento Seguro
9.2 - Autenticação, Autorização e Compliance
9.3 - Identidade e Gerenciamento de Acesso para Aplicações
9.4 - Testes de Invasão para Aplicações

CSA


10 - Gerenciamento de Chaves e Encriptação
10.1 - Encrip. de Dados em Trânsito
10.2 - Encrip. de Dados em Repouso
10.3 - Encrip. de Backup de Dados
10.4 - Armazenamento Seguro de Chaves
10.5 - Acesso ao Armazenamento de Chaves
10.6 - Backup e Recuperação de Chaves
11 - Identidade e Gerenciamento de Acesso
11.1 - Provisionamento de Identidade
11.2 - Autenticação
11.3 - Federação
11.4 - Autorização e Gerenciamento de Perfis de Usuário
12 - Virtualização
12.1 - Arquitetura do Hypervisor
13 - Segurança como Serviço
13.1 - Ubiquidade do Serviço
13.2 - Preocupações na Implementação
13.3 - Benefícios de se Implementar Seg. como Serv.
13.4 - Diversidade de Serviços que Podem ser Class. como Seg. como Serv.

ENISA


Questões de Segurança na Nuvem - ENISA
Políticas e Organizacionais
1 - Lock-in
2 - Governança
3 - Compliance
4 - Perda de Reputação de Negócios devido a co-Inquilinos
5 - Finalização ou Falha do Serviço de Nuvem
6 - Aquisição de Provedor de Nuvem
7 - Falha de Cadeia de Fornecimento
Questões Técnicas
8 - Exaustão de Recursos
9 - Isolamento de Falhas
10 - Ameaças Internas
11 - Gerenciamento de Interface
12 - Interceptação de Dados em Trânsito
13 - Vazamento de Dados em Upload e Download
14 - Exclusão Sem Efeito ou Insegura dos Dados
15 - Negação de Serviço Distribuída
16 - Negação de Serviço Economica
17 - Perda de Chaves de Encriptação
18 - Captação de Sondas ou Scans Maliciosos
19 - Comprometimento de Motor de Serviço
20 - Conflitos entre Endurecimento de Procedimentos do Cliente e o Ambiente de Nuvem
Aspectos Legais
21 - Descoberta Eletrônica e Intimações Judiciais
22 - Riscos de Mudanças de Jurisdição
23 - Risco de Proteção dos Dados
24 - Riscos de Licenciamento

Comparativo

Questões políticas, organizacionais e legais	Subtópicos	NIST	CSA	ENISA
1 - Governança e Gerenciamento de Risco		Abordado	Abordado	Abordado
2 - Conformidades e Auditoria	2.1 - Conformidades de Leis e Regulamentos	Abordado	Abordado	Abordado
	2.2 - Conformidades de Localização dos Dados	Abordado	Abordado	Abordado
3 - Aspectos legais		Abordado	Abordado	Abordado
4 - Ameaças Internas		Abordado	Abordado	Abordado
5 - Tratamento dos Dados	5.1 - Proteção dos Dados a respeito dos Usuários	Abordado	n.a.	n.a.
	5.2 - Propriedade Intelectual	Abordado	Abordado	Abordado
	5.3 - Disponibilidade dos Dados p/ Análise Forense	Abordado	Abordado	Abordado
6 - Relatórios de Acidentes		Abordado	Abordado	Abordado
7 - Gerenciamento de Patch		Abordado	Abordado	Abordado
8 - Vistorias	8.1 - Vistoria do Provedor	Abordado	Abordado	Abordado
	8.2 - Vistoria das Dependências do Provedor	Abordado	Abordado	Abordado

Questões Técnicas	Subtópicos	NIST	CSA	ENISA
1 – Disponibilidade	1.1 - Interrupções	Abordado	Abordado	Abordado
	1.2 - Exaustão de recursos	n.a.	Abordado	Abordado
	1.3 - Ameaças de disponibilidades por ataques de DoS	Abordado	n.a.	Abordado
	1.4 - Ameaças por compartilhamento de dados	Abordado	Abordado	Abordado
2 – Portabilidade	2.1 - Portabilidade de fados	Abordado	Abordado	Abordado
	2.2 - Portabilidade de imagens de VMs	n.a.	Abordado	Abordado
	2.3 - Portabilidade de aplicações	Abordado	Abordado	Abordado
3 - Gerenciamentos de dados	3.1 – Isolamento	Abordado	Abordado	Abordado
	3.2 - Backup e recuperação	Abordado	Abordado	Abordado
	3.3 – Exclusão	Abordado	Abordado	Abordado
	3.4 – Cifração/cifragem	Abordado	Abordado	Abordado
	3.5 - Gerenciamento de chaves	Abordado	Abordado	Abordado
	3.6 - Verificação de integridade	Abordado	Abordado	n.a.
4 - Identidade e gerenciamento de acesso	4.1 - Provisionamento e desprovisionamento de identidade	n.a.	Abordado	Abordado
	4.2 - Federação de identidade	Abordado	Abordado	Abordado
	4.3 - Autenticação	Abordado	Abordado	Abordado
	4.4 - Autorização e controle de acesso	Abordado	Abordado	Abordado
5 - Segurança de aplicação	5.1 - Proteção do cliente	Abordado	Abordado	Abordado
	5.2 - Proteção do servidor	Abordado	Abordado	Abordado
	5.3 - Proteção da imagem da VM	Abordado	Abordado	Abordado
	5.4 - Proteção dos arquivos de log	n.a.	Abordado	Abordado
6 – Virtualização	6.1 - Proteção do hypervisor	Abordado	Abordado	Abordado
	6.2 - Proteção do sistema operacional visitante	Abordado	Abordado	Abordado
	6.3 - Proteção da rede virtual	Abordado	Abordado	Abordado

Referências

- Slides elaborados a partir de:

- Markus Endler – Introdução à Computação em Nuvem. PUC-RJ.
- Fernando Seabra Chirigati – Computação em Nuvem. UFRJ
- Normam Wilde e Thomas Wuber. Virtualization and Cloud Computing.
- Miers et al. Análise de Segurança para Soluções de Computação em Nuvem. Mini-curso do SBRC 2014.