Soluções SmartCloudPT

Segurança na Cloud

Fiabilidade e Disponibilidade

Cláudia Pais
Direção de Gestão de Produto

Outubro 2013

1 MODELO DE SERVIÇOS

2 TOP AMEAÇAS

3 SEGURANÇA PT

1 MODELO DE SERVIÇOS

Cloud Computing - Paradigma tecnológico em que recursos de TI/SI e respetiva informação estão residentes em Data Centers remotos, sendo disponibilizados na rede como um serviço.

SaaS
Software-as-a-service

Google · Microsoft · YAHOO! MAIL · UNISYS

PaaS
Platform-as-a-service

force.com platform as a service · Windows Azure · ORACLE

IaaS
Infrastructure-as-a-service

amazon web services · rackspace · SkyDrive · IBMSmartCloud · flexiant · Xdrive

- Funcionalidade self-service (provisão dinâmica)
- Partilha de recursos (virtualização do hardware)
- Acesso constante à rede (em qualquer momento a qualquer hora)
- Elasticidade (flexível e facilmente escalável)
- Serviço pay-per-use (faturação por utilização)

1 MODELO DE SERVIÇOS

Segurança na Cloud

INTEGRIDADE

Prevenção contra a modificação e/ou destruição não autorizada de Informação, salvaguardando a respectiva fiabilidade e origem.

CONFIDENCIALIDADE

Prevenção contra o acesso e/ou divulgação não autorizados de Informação.

DISPONIBILIDADE

Garantia do acesso autorizado à Informação sempre e na medida do necessário.

AUDITING

Garantia do registo do acesso às plataformas e à Informação, sobre o utilizador, data e hora da ação.

1 MODELO DE SERVIÇOS

2 TOP AMEAÇAS

3 SEGURANÇA PT

2 TOP AMEAÇAS

5º (2010)

1

VIOLAÇÃO DE DADOS

5º (2010)

2

PERDA DE DADOS

Ameaça

Dados sensíveis são acedidos por pessoas não autorizadas / concorrência.

Prevenção

Cifrar os dados para mitigar o risco de violação dos mesmos.

Ameaça

Intrusão de hackers; Eliminação acidental pelo fornecedor; Catástrofes como incêndios e tremores de terra.

Prevenção

Medidas de salvaguarda de dados (Backup) com politicas de retenção; Localização do Data Center.

2 TOP AMEAÇAS

6º (2010)

3

SEQUESTRO DE CONTA OU TRÁFEGO

5º (2010)

4

APIs INSEGURAS

Ameaça

Passwords roubadas; Espiar a atividade e operações; Manipular dados; Redirecionar clientes para sites maliciosos.

Prevenção

Não permitir a partilha entre utilizadores das credenciais de acesso a serviços na Cloud; Implementar, sempre que possível, autenticação forte com multi-factor.

Ameaça

A utilização de APIs para acrescentar serviços às soluções aumenta o risco de ocorrência de intrusões.

Prevenção

Assegurar que o portal de interação do cliente com os serviços Cloud é seguro e não apresenta vulnerabilidades de software.

2 TOP AMEAÇAS

N/A (2010)

5

NEGAÇÃO DE SERVIÇO

3º (2010)

6

ADMINISTRAÇÃO CLOUD MALICIOSA

Ameaça

Os ataques de DDoS (*Distributed Denial of Service*) são hoje simples de executar através de *Botnets* e bastante eficazes.

Prevenção

Defender a infraestrutura à entrada do link de Internet, de modo a que um ataque DDoS não congestione a conectividade e provoque a perda parcial ou total do serviço.

Ameaça

Os administradores da nuvem, com acesso aos dados, podem usar os privilégios que possuem para comprometer dados.

Prevenção

Conjunto limitado de administradores de sistemas, devidamente identificados e com acordos de confidencialidade assinados.

2 TOP AMEAÇAS

1º (2010)

7

ABUSO DE SERVIÇOS CLOUD

7º (2010)

8

DILIGÊNCIA INSUFICIENTE

Ameaça

Recursos computacionais usados para fins ilegais: quebrar chaves de cifragem; realizar ataques DDoS; distribuir software malicioso.

Prevenção

Ter uma equipa especializada em Segurança de Informação com ferramentas de SIEM*, para análises forenses a eventos de segurança de Informação.

*SIEM: Security Information and Event Management

Ameaça

Risco de empresas migrarem para a nuvem sem se aperceberem suficientemente das implicações.

Prevenção

Considerar qual é a disponibilidade oferecida, qual a possibilidade de indeminização em caso de falha e qual é a facilidade de mudar para outro fornecedor.

2 TOP AMEAÇAS

4º (2010)

9

VULNERABILIDADE TECNOLOGIAS PARTILHADAS

Ameaça

A partilha de recursos computacionais pode permitir que uma vulnerabilidade seja explorada.

Prevenção

Monitorizar o ambiente para detetar atividades e alterações não autorizadas; Patching e resolução de vulnerabilidades; Auditorias de configuração.

1 MODELO DE SERVIÇOS

2 TOP AMEAÇAS

3 SEGURANÇA PT

3 SEGURANÇA PT

A PT construiu o mais avançado Data Center da Europa, reforçando significativamente a capacidade atual.

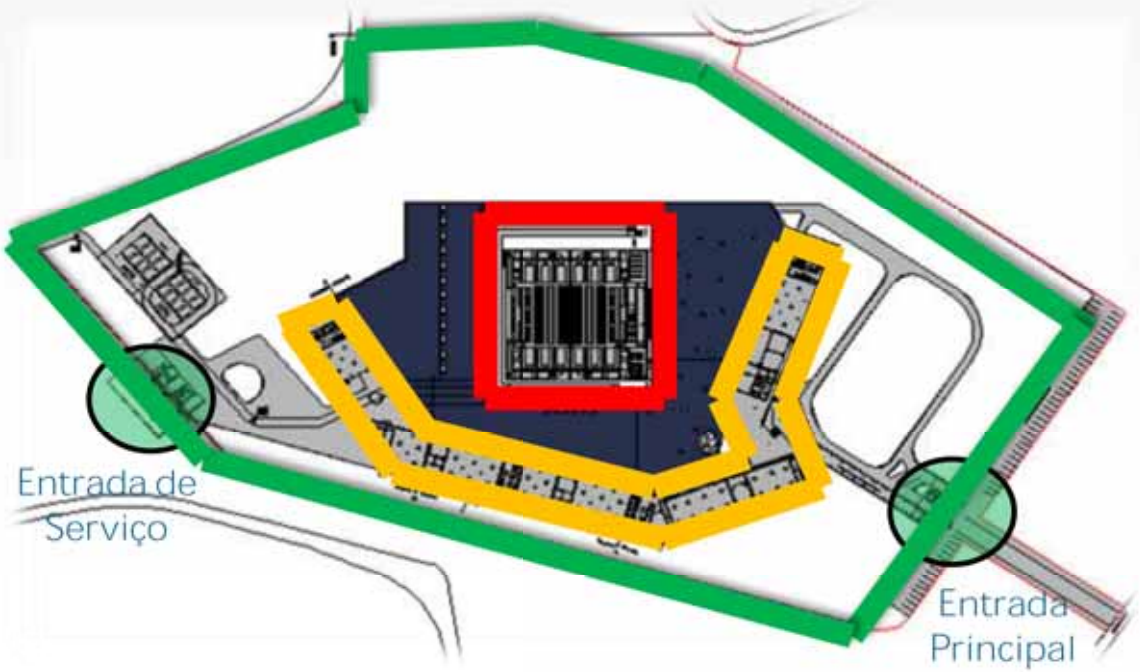
Capacidade Anterior

Nova Capacidade

Soluções SmartCloudPT

3 SEGURANÇA PT

Segurança Física



Perímetro Exterior
1º nível de segurança
Intrusão, Desordem Pública e Vandalismo.

Edifício de Suporte
2º nível de segurança
Fogo, Inundações; Roubo/Intrusão; Ameaça de Bomba; Desordem Pública e Vandalismo

Data Center
3º nível de segurança
Fogo, Inundações; Roubo/Intrusão; Ameaça de Bomba;

Certificações e Melhores Práticas

Uptime Institute

O *Uptime Institute* apresenta-se como organização de referência internacional na certificação de Data Centers, considerando a resiliência, redundância e processos de manutenção da infraestrutura.

O Data Center da Covilhã obteve a Certificação Uptime Tier III, garantindo assim o funcionamento contínuo pelo desenho da infraestrutura através do princípio da redundância N+1, sendo a TI alimentada por 2 caminhos independentes e redundantes , permitindo uma disponibilidade de 99,98%

ISO 9001 ISO 27001 ITIL ISO/IEC 20000

A Portugal Telecom está certificada com a ISO9001, ISO20000 e a ISO27001. São também seguidas as boas práticas definidas pela ITIL.

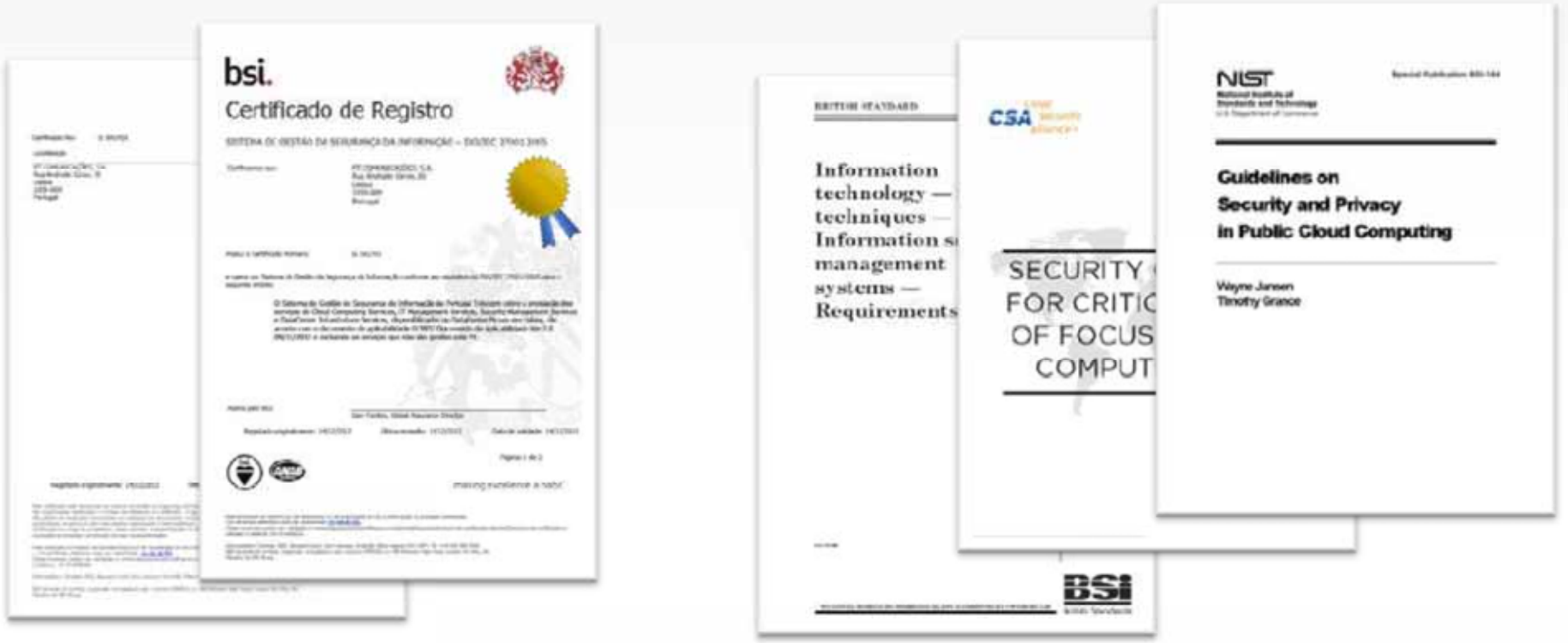
LEED

A USGBC é uma Organização Americana responsável pelo processo de certificação LEED. Esta certificação traduz o mérito ambiental de um edifício ou campus, considerando todo o seu ciclo de vida e ecosistema.

Standard *Silver* *Gold* *Platinium*

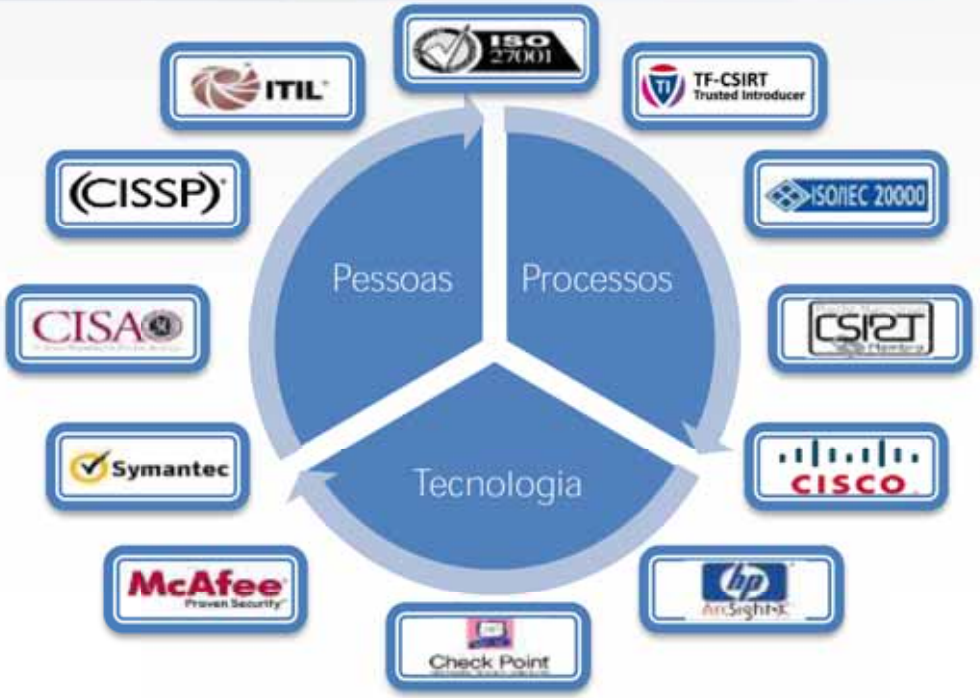
A LEED apresenta 4 certificações distintas

A PT tem os seus sistemas certificados e aplica as melhores práticas de segurança na cloud.



Portfólio de Segurança integra as pessoas, os processos e a tecnologia.

- Formação especializada
- Certificação em Segurança
- Equipa 24x7 SOC (Security Operations Center)



- Modelos de gestão de serviço certificados
- PT pertence ao CSIRT PT (Computer Security Incident Response Team)
- Tecnologia State of the art SIEM (Security Information Event Management)

- Principais parceiros

Atuação abrangente nas áreas da Segurança Física, Lógica e Legal

FÍSICA

- Gestão e controlo de acessos, perímetros de segurança
- Condições ambientais

LÓGICA

- QoS rede
- Encriptação de dados
- Integração AD
- SOC

LEGAL

- Modelos contratuais
- Integridade
- Portabilidade

CONTINUIDADE DO NEGÓCIO

Plataformas redundantes entre DCs PT, Disaster & Recovery e Salas de Business Continuity

INVESTIGAÇÃO, FORMAÇÃO, CERTIFICAÇÕES

ISO 20000, ISO 27001, CsirtPT, PT Security Labs

3 SEGURANÇA PT

A Portugal Telecom possui a maior rede nacional de telecomunicações e todas as condições para ser líder nos serviços IT & Cloud Computing.

REDE NACIONAL DE DATA CENTERS

- Aumento da rede nacional de Data Centers disponibilizando serviços com elevada disponibilidade, redundância, e escalabilidade.

REDE DE DADOS DE NOVA GERAÇÃO

- Rede de dados suportada em infraestrutura de fibra de alto débito, com elevada capilaridade e prioritização de tráfego.

PLATFORMA DE SERVICE

- Plataformas com operação multi-tenant, unificação de faturação e de portais de self-care.

CONHECIMENTOS SEGURANÇA

- Credibilidade na implementação de politicas de segurança e sistemas de informação.

3 SEGURANÇA PT

PT tem os melhores parceiros globais que confiam na capacidade de inovar e crescer no mercado de TIC. Com estes modelos de parcerias é possível uma rápida e eficaz resposta às necessidades do mercado.

Portfólio Segurança

O Portfólio de Segurança integrado com soluções de Disaster Recovery e Business Continuity permitem uma proteção holistica.

Os Serviços Modulares potenciam a costumização das soluções com o foco centrado nos reais requisitos dos clientes.

A Portugal Telecom é membro da rede nacional de CSIRT e da rede Trusted Introducer para cooperação internacional.

TF-CSIRT Trusted Introducer

Rede Nacional CSIRT Membro

3 SEGURANÇA PT

Portfólio Segurança

SERVIÇOS

- Gestão de Incidentes de Segurança.
- Alarmes de Incidentes de Segurança.
- Relatórios de Segurança.
- Correlação de Eventos.

CARACTERISTICAS

- Supervisão de eventos de segurança.
- Diferentes alarmes para diferentes severidades.
- Relatórios periodicos que simplificam a análise de eventos.
- Análise de eventos por equipas especializadas.

VANTAGENS

- Escalabilidade
- Holistico
- Experiência
- Excelência
- Simplicidade

Soluções SmartCloudPT

Segurança na Cloud

Fiabilidade e Disponibilidade

Cláudia Pais
Direção de Gestão de Produto

Outubro 2013