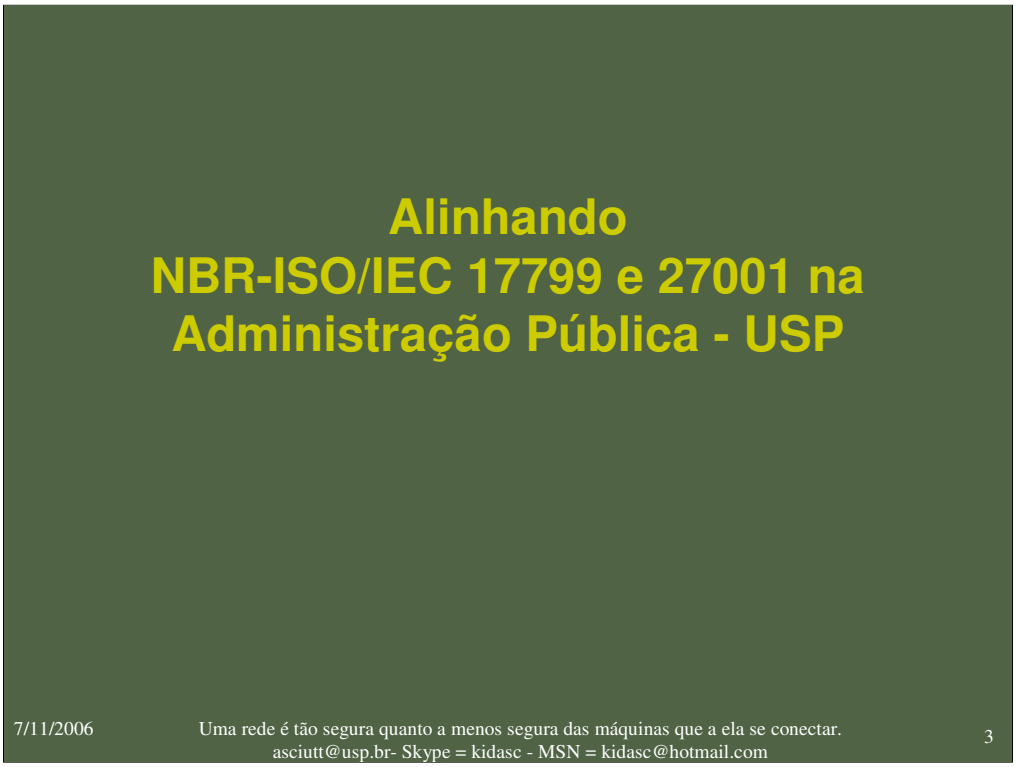
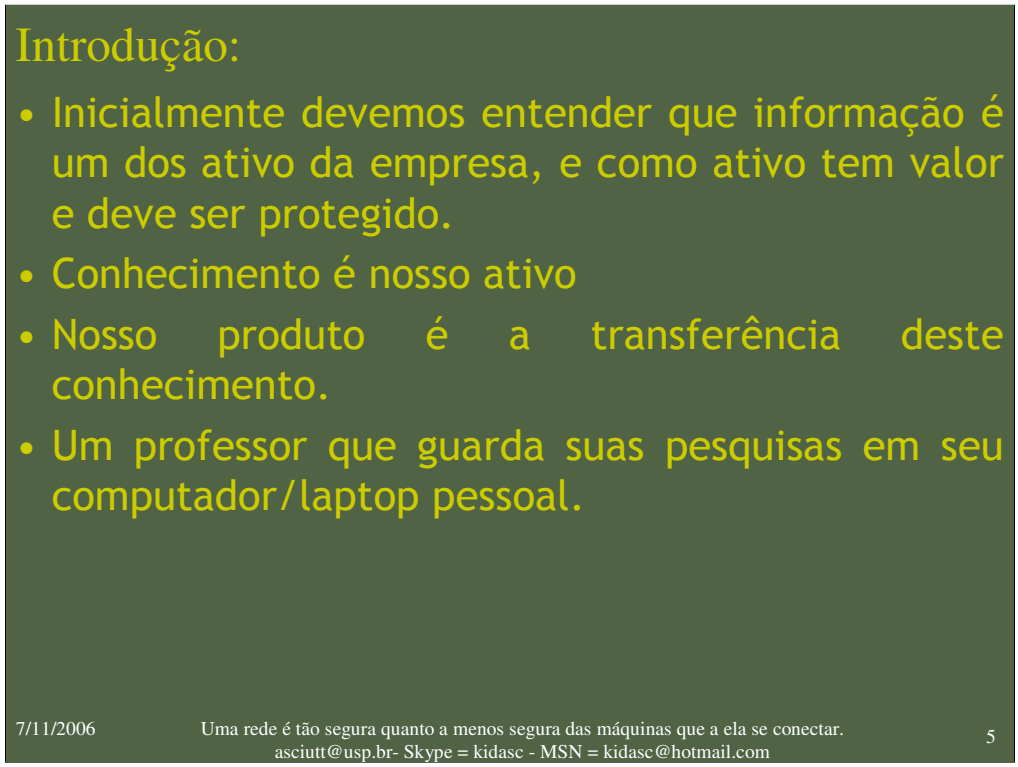

Alinhando
NBR-ISO/IEC 17799 e 27001 na
Administração Pública - USP
7/11/2006
Uma rede é tão segura quanto a menos segura das máquinas que a ela se conectar.
asciutt@usp.br- Skype = kidasc - MSN = kidasc@hotmail.com
3

Bom dia a todos,

Falarei sobre a Norma vigente e apresentarei uma proposta para implantação aqui na USP.

O assunto é muito amplo, portanto Farei uma apresentação rápida da norma.

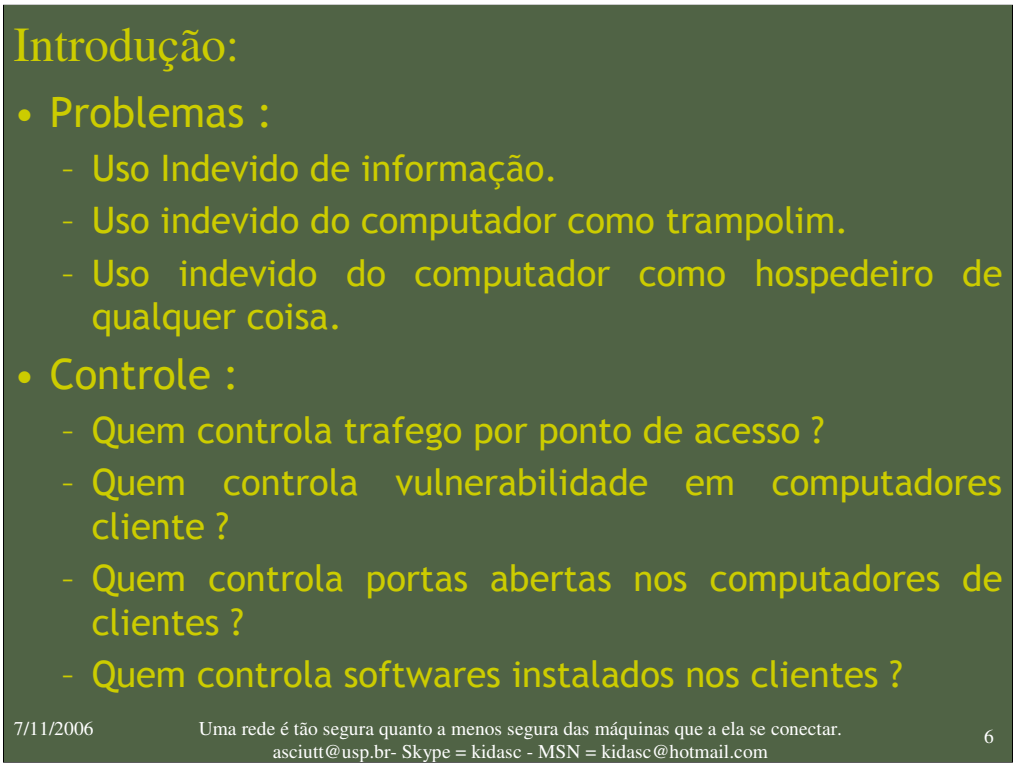
Vou procurar aterme mais ao plano de ação, e as questões que vocês apresentarem.



Inicialmente devemos entender que informação é um dos ativo da empresa, e como ativo tem valor e deve ser protegido. Pessoas, seus conhecimentos e o que ela representa, também são ativos. Marca e Imagem também são ativos.

Aqui, na USP, o conhecimento é nosso ativo, e o nosso produto é a transferência deste conhecimento. Parte na nossa missão também e conhecer mais.

Um professor que guarda suas pesquisas em seu computador/laptop pessoal não nos dando a administração, é o mesmo que irá nos culpar caso ocorra qualquer problema com esse equipamento.



Problemas :

Uso Indevido de informação.

Uso indevido do computador como trampolim.

Uso indevido do computador como hospedeiro de qualquer coisa.

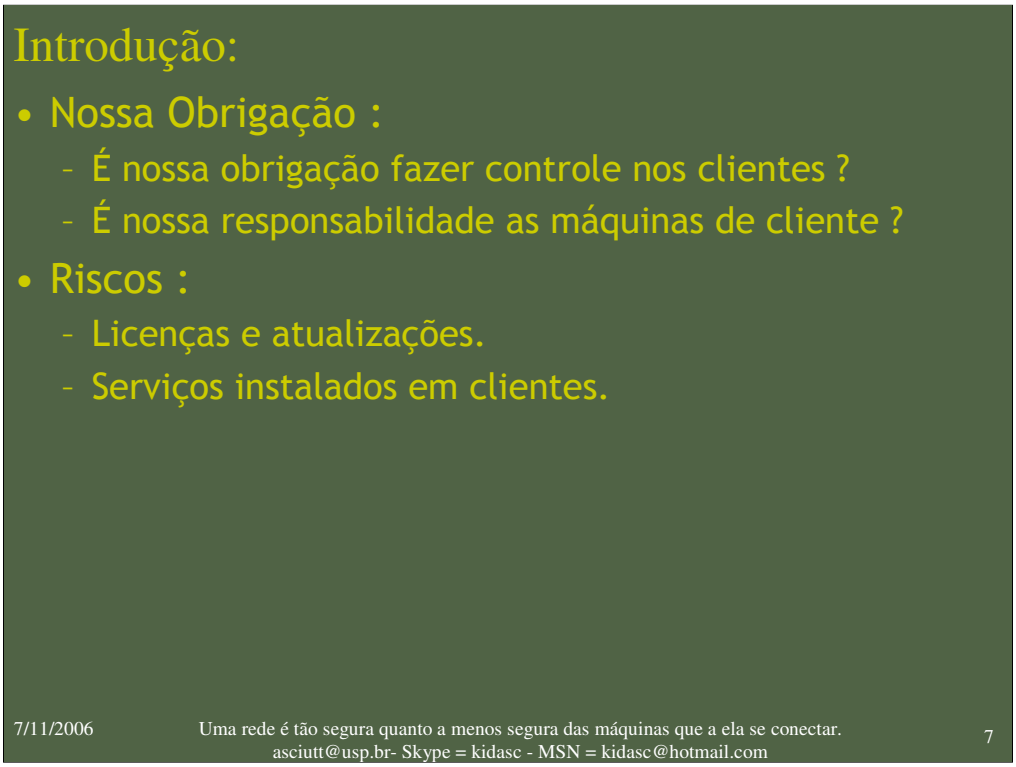
Controle :

Quem controla trafego por ponto de acesso ?

Quem controla vulnerabilidade em computadores cliente ?

Quem controla portas abertas nos computadores de clientes ?

Quem controla softwares instalados nos clientes ?



Nossa Obrigação :

É nossa obrigação fazer controle nos clientes ?

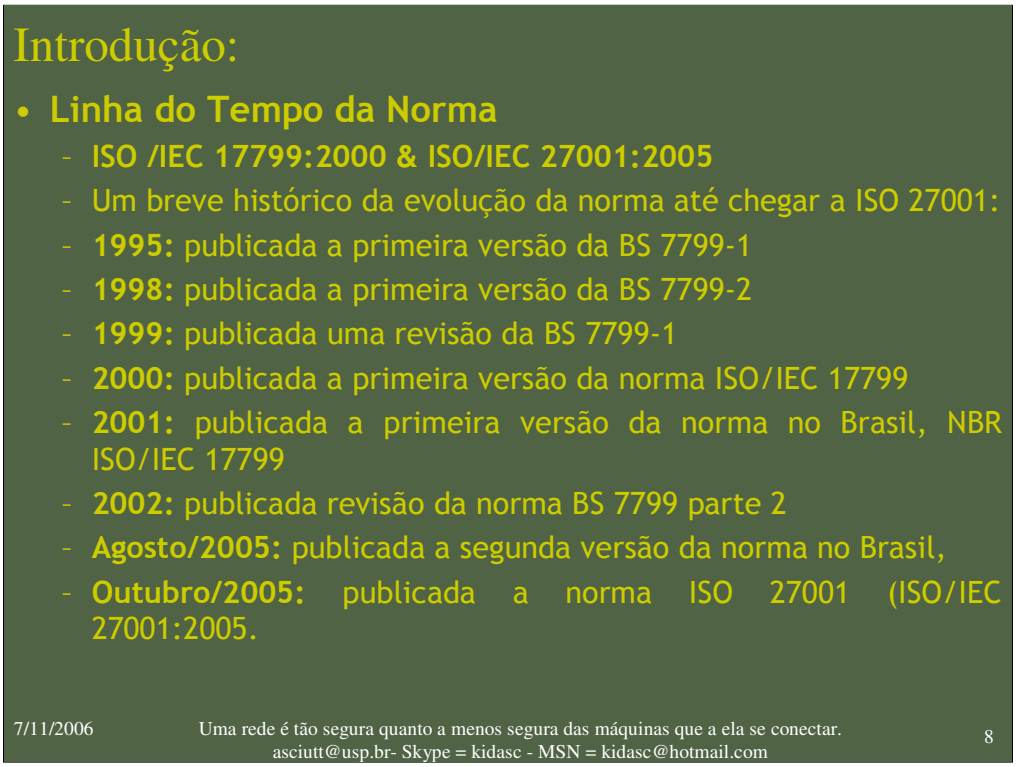
É nossa responsabilidade as máquinas de cliente ?

Riscos :

Licenças e atualizações.

Serviços instalados em clientes.

Por definição, o risco é a ameaça de que um novo evento afete a habilidade da empresa em atingir seus objetivos e suas estratégias de negócios. Não há empresa próspera que não corra riscos. A expansão, bem como a manutenção de um negócio, pressupõe que os riscos existam e devam ser entendidos como parte integrante do negócio.



Linha do Tempo da Norma

ISO /IEC 17799:2000 & ISO/IEC 27001:2005

Um breve histórico da evolução da norma até chegar a ISO 27001:

- 1995: publicada a primeira versão da BS 7799-1 (BS 7799-1:1995 - Tecnologia da Informação - **Código de prática para gestão da segurança da informação**)

- 1998: publicada a primeira versão da BS 7799-2 (BS 7799-2:1998 - Sistema de gestão da Segurança da Informação - **Especificações e guia para uso**)

- 1999: publicada uma revisão da BS 7799-1 (BS 7799-1:1999 - Tecnologia da Informação - **Código de prática para gestão da segurança da informação**)

- 2000: publicada a primeira versão da norma ISO/IEC 17799 (ISO/IEC 17799:2000 - Tecnologia da Informação - **Código de prática para gestão da segurança da informação** também referenciada como BS ISO/IEC 17799:2000)

- 2001: publicada a primeira versão da norma no Brasil, NBR ISO/IEC 17799 (NBR ISO/IEC 17799:2001 - Tecnologia da Informação - Código de prática para gestão da segurança da informação)

- 2002: publicada revisão da norma BS 7799 parte 2 (BS7799-2:2002 - **Sistema de gestão da Segurança da Informação - Especificações e guia para uso**).

- Agosto/2005: publicada a segunda versão da norma no Brasil, NBR ISO/IEC 17799 (NBR ISO/IEC 17799:2005 - Tecnologia da Informação - **Código de prática para gestão da segurança da informação**);

- Outubro/2005: publicada a norma ISO 27001 (ISO/IEC 27001:2005 - Tecnologia da Informação - **Técnicas de segurança - Sistema de gestão da Segurança da Informação - Requisitos**).

Introdução:

- Relembrando a **ABNT NBR ISO/IEC-17799** (Norma anterior)

Norma Anterior : NBR/ISO-17.799	Norma Atual : NBR/ISO-17.799-2005
A norma nacional de segurança de informação é dividida nos 10 macros controles:	O novo padrão agora contém 11 capítulos principais renomeados e reorganizados. Os novos capítulos são:
Política de Segurança;	Políticas de Segurança
Segurança Organizacional;	Organizando a Segurança da Informação
Classificação e Controle dos Ativos da Informação;	Gerenciamento de ativos
Segurança em Pessoas;	Segurança dos Recursos Humanos
Segurança Física e do Ambiente;	Segurança Física e Ambiental
Gerenciamento de Operações e Comunicações;	Gerenciamento das Comunicações e Operações
Controle de Acesso;	Controle de Acessos
Desenvolvimento da Segurança de Sistemas;	**Aquisição**, Desenvolvimento e **Manutenção** de Sistemas de Informação
	Gerenciamento de Incidentes na Segurança da Informação
Gestão da Continuidade do Negócio;	Gerenciamento da Continuidade do Negócio
Conformidade.	Conformidade.

7/11/2006 Uma rede é tão segura quanto a menos segura das máquinas que a ela se conectar. asciutt@usp.br- Skype = kidasc - MSN = kidasc@hotmail.com 9

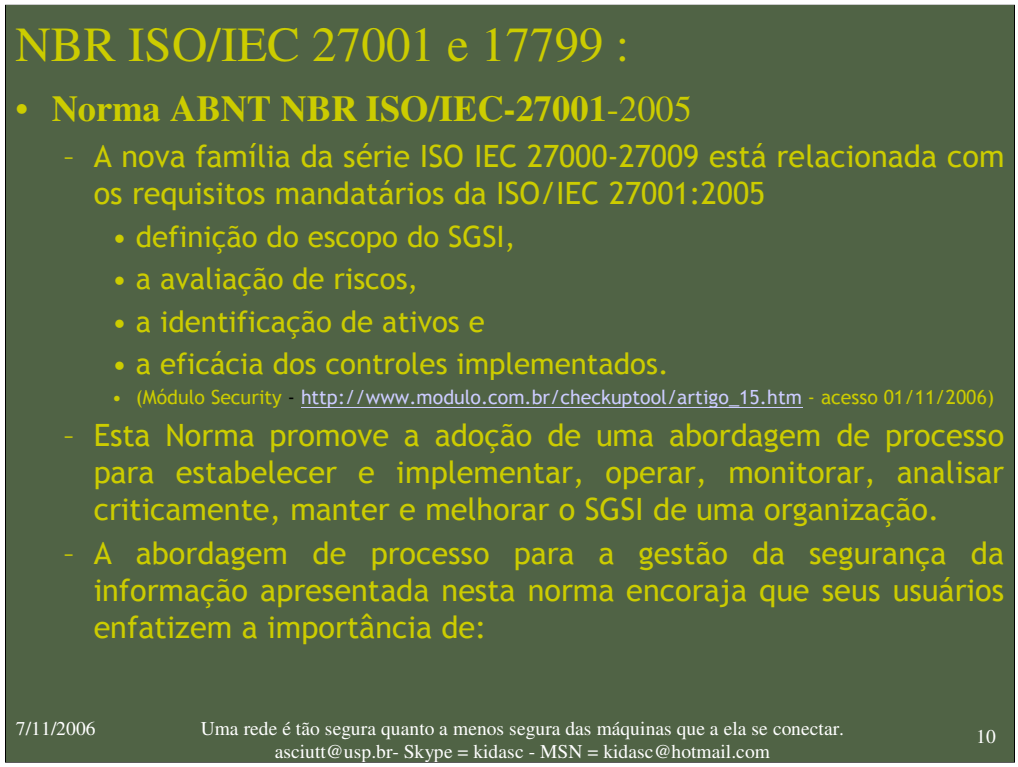
Criado dois focos novos no escopo da ação:

Desenvolvimento de Segurança de sistemas foi ampliado com:

Aquisição e Manutenção

Introduzido o Gerenciamento de Incidente

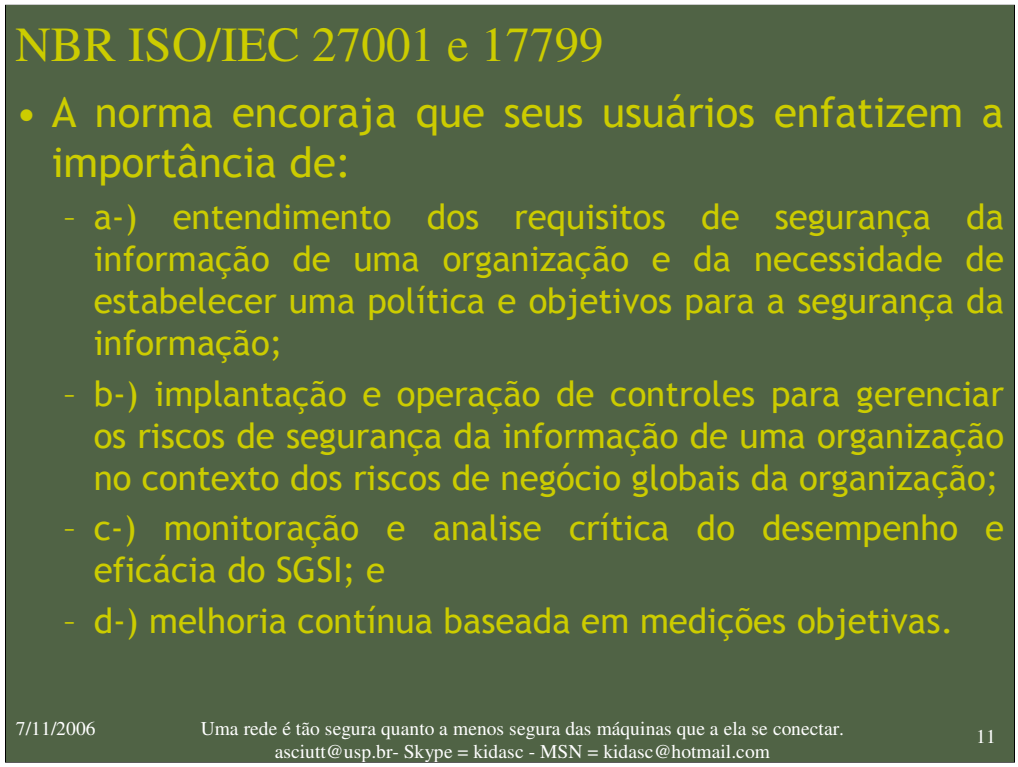
No restante houveram melhorias no geral e ampliação dos focos de atuação.



A nova família da série ISO IEC 27000-27009 está relacionada com os requisitos mandatários da ISO/IEC 27001:2005, como, por exemplo, a definição do escopo do Sistema de Gestão da Segurança da Informação, a avaliação de riscos, a identificação de ativos e a eficácia dos controles implementados. (Módulo Security - http://www.modulo.com.br/checkuptool/artigo_15.htm - acesso 01/11/2006)

Esta Norma promove a adoção de uma abordagem de processo para estabelecer e implementar, operar, monitorar, analisar criticamente, manter e melhorar o SGSI de uma organização.

A abordagem de processo para a gestão da segurança da informação apresentada nesta norma encoraja que seus usuários enfatizem a importância de:



A abordagem de processo para a gestão da segurança da informação apresentada nesta norma encoraja que seus usuários enfatizem a importância de:

a-) entendimento dos requisitos de segurança da informação de uma organização e da necessidade de estabelecer uma política e objetivos para a segurança da informação;

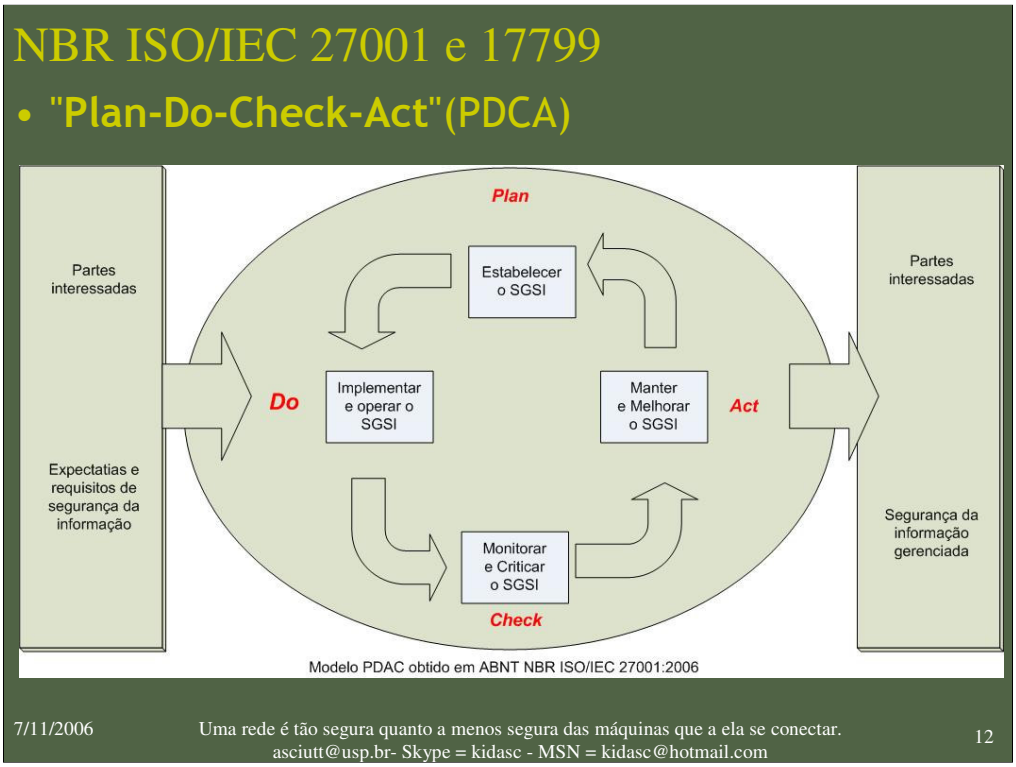
b-) implantação e operação de controles para gerenciar os riscos de segurança da informação de uma organização no contexto dos riscos de negócio globais da organização;

c-) monitoração e analise crítica do desempenho e eficácia do SGSI; e

d-) melhoria contínua baseada em medições objetivas.

SGSI

O SGSI é projetado para assegurar a seleção de controles de segurança adequados e proporcionados para proteger os ativos de informação e propiciar confiança às partes interessadas.

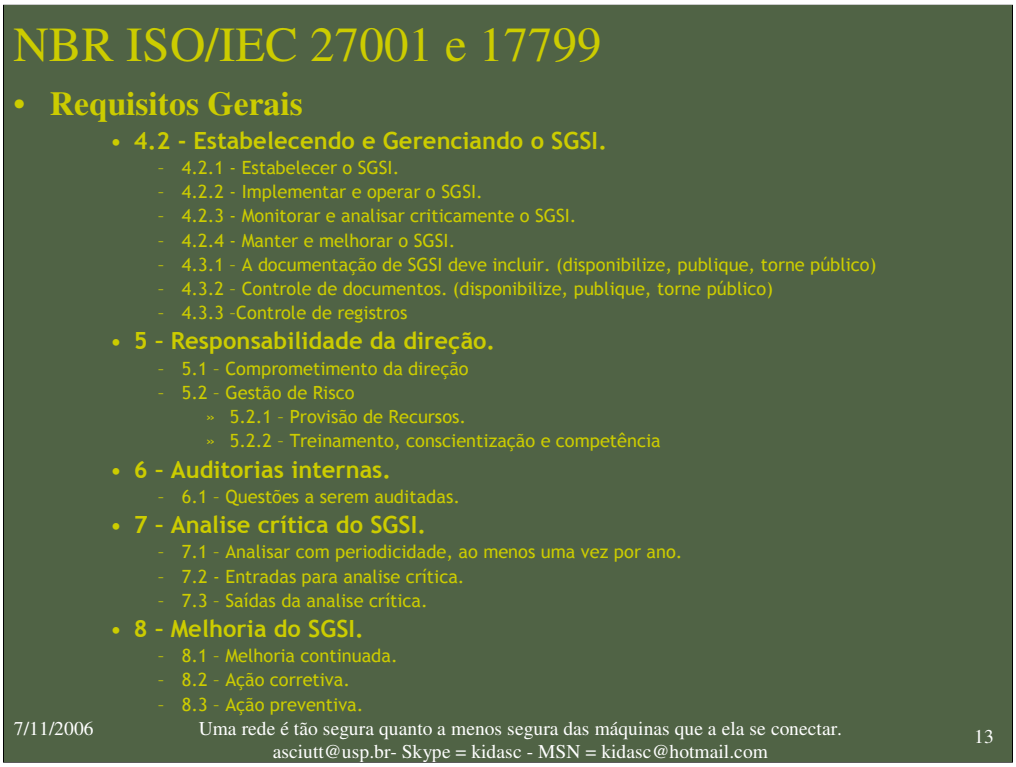


"***Plan***" – Planejar – Estabelecer o SGSI – Estabelecer a política, objetivos, processos e procedimentos do SGSI, relevantes para a gestão de riscos e a melhoria da segurança da informação para produzir resultados de acordo com as políticas e objetivos globais de uma organização.

"***Do***" – Fazer – Implementar e Operar o SGSI - Implementar e operar a política, controles, processos e procedimentos do SGSI.

"***Check***" – Checar/Monitorar/Analisar Criticamente – Avaliar e, quando aplicável, medir o desempenho de um processo frente à política, objetivos e experiências prática do SGSI e apresentar os resultados para a analise crítica pela direção.

"***Act***" – Agir – Manter e melhorar o SGSI – Executar as ações corretivas e preventivas, com base nos resultados da auditoria interna do SGSI e da análise crítica pela direção ou outra informação pertinente, para alcançar a melhoria contínua do SGSI.



Requisitos gerais

4.2 - Estabelecendo e Gerenciando o SGSI.

4.2.1 - Estabelecer o SGSI.

a-) Definir um escopo.

b-) Definir uma política.

c-) Definir a abordagem de analise/avaliação de riscos da organização.

(ex. veja [ISO/IEC 13335-3])

d-) Identificar os Riscos.

e-) Identificar e avaliar os riscos.

f-) Identificar e avaliar as opções para o tratamento de riscos.

g-) Selecionar objetos de controle e controles para o tratamento de riscos.

h-) Obter aprovação da direção dos riscos residuais propostos.

i-) Obter autorização da direção para implantar e operar o SGSI.

i-) Preparar uma declaração de aplicabilidade.

4.2.2 - Implementar e operar o SGSI.

a-) Formular um plano de tratamento de risco.

b-) Implementar o plano de tratamento de risco.

c-) Implementar controles selecionados.

d-) Definir como medir a eficácia dos controles.

e-) Implementar programas de conscientização e treinamento. (Brigada).

f-) Gerenciar as operações do SGSI.

g-) Gerenciar os recursos do SGSI.

h-) Implementa procedimentos e outros controles.

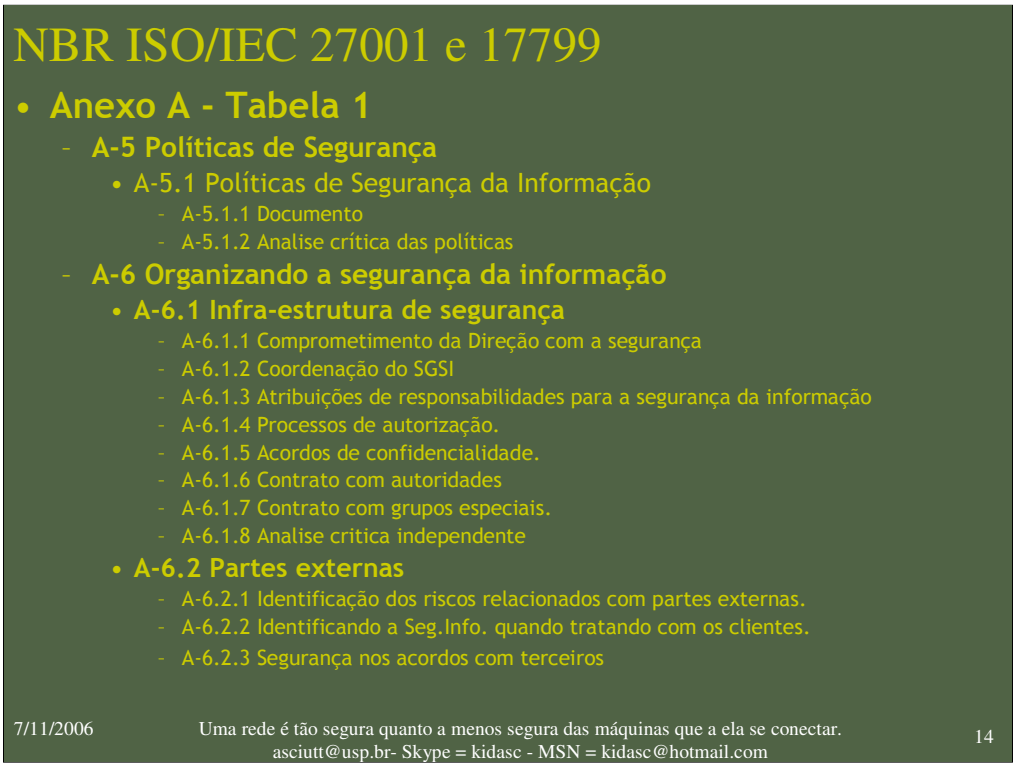
4.2.3 - Monitorar e analisar criticamente o SGSI.

a-) Executar procedimentos de monitoração.

b-) Analisar analises críticas.

c-) Implementar controles selecionados.

d-) Analisar criticamente as analises/avaliações de riscos.



Anexo A

Tabela 1

A-5 Políticas de Segurança

A-5.1 Políticas de Segurança da Informação

A-5.1.1 Documento

Gerar um documento com as políticas, submetendo a aprovação pela diretoria e divulgado à todos.

A-5.1.2 Analise crítica das políticas

Reveja periodicamente estas políticas refazendo-as quando necessário.

A-6 Organizando a segurança da informação

A-6.1 Infra-estrutura de segurança

A-6.1.1 Comprometimento da Direção com a segurança

A direção deve apoiar ativamente as políticas adotadas.

A-6.1.2 Coordenação do SGSI

Mantenha um grupo interdisciplinar na elaboração e manutenção do SGSI

A-6.1.3 Atribuições de responsabilidades para a segurança da informação

Definir com clareza as responsabilidade.

A-6.1.4 Processos de autorização.

Ter um processo claro, e documentado sobre a gestão da segurança.

A-6.1.5 Acordos de confidencialidade.

Ter documentado e divulgado os acordos de confidencialidade.

A-6.1.6 Contrato com autoridades

Contrato apropriados com autoridades relevantes devem ser mantidos. (certificadoras, auditoras)

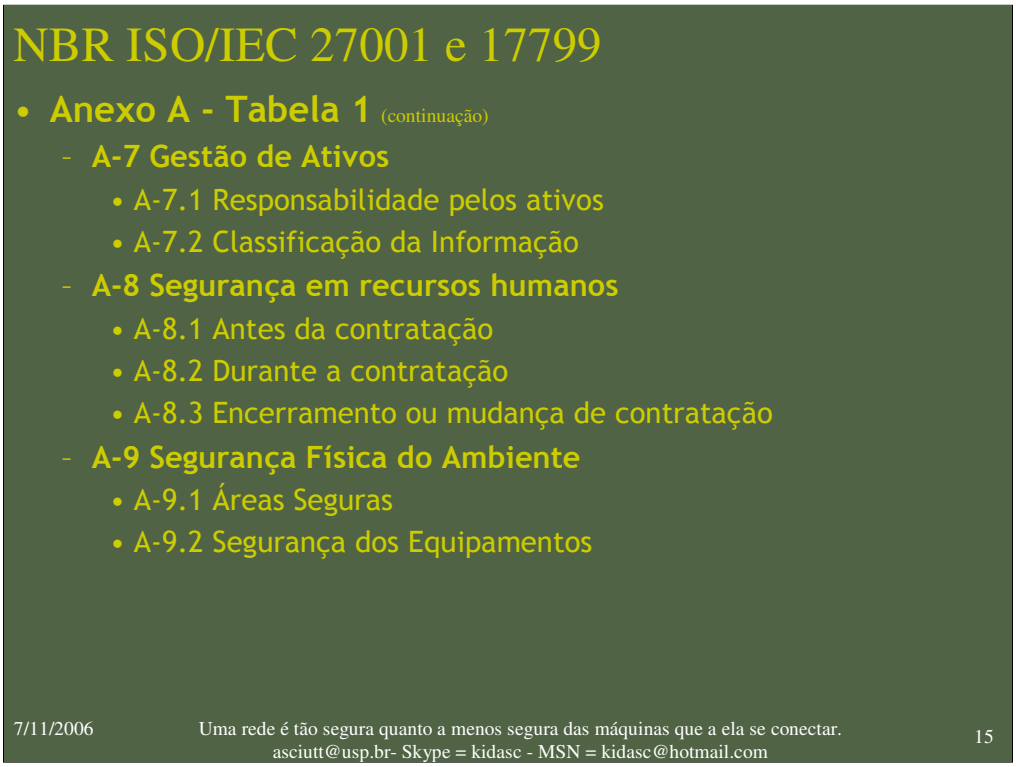
A-6.1.7 Contrato com grupos especiais.

Contrato apropriados com grupos de interesses especiais ou outros fóruns ou associações profissionais.

A-6.1.8 Analise critica independente

O enfoque da organização para gerenciar a segurança da informação e a sua implementação. (Controles, Objetivos dos controles, Políticas, Processos, procedimentos, etc...)

A-6.2 Partes externas



Anexo A

Tabela 1

.....

A-7 Gestão de Ativos

A-7.1 Responsabilidade pelos ativos

A-7.2 Classificação da Informação

A-8 Segurança em recursos humanos

A-8.1 Antes da contratação

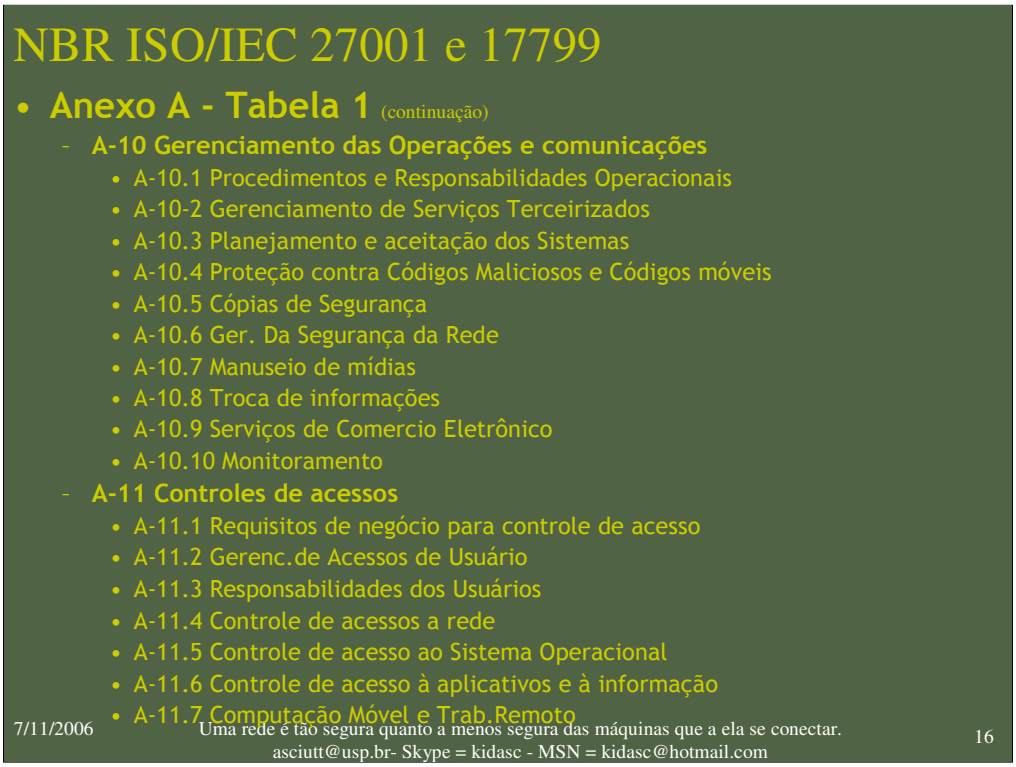
A-8.2 Durante a contratação

A-8.3 Encerramento ou mudança de contratação

A-9 Segurança Física do Ambiente

A-9.1 Áreas Seguras

A-9.2 Segurança dos Equipamentos



Anexo A

Tabela 1

.....

A-10 Gerenciamento das Operações e comunicações

A-10.1 Procedimentos e Responsabilidades Operacionais

A-10-2 Gerenciamento de Serviços Terceirizados

A-10.3 Planejamento e aceitação dos Sistemas

A-10.4 Proteção contra Códigos Maliciosos e Códigos móveis

A-10.5 Cópias de Segurança

A-10.6 Ger. Da Segurança da Rede

A-10.7 Manuseio de mídias

A-10.8 Troca de informações

A-10.9 Serviços de Comercio Eletrônico

A-10.10 Monitoramento

A-11 Controles de acessos

A-11.1 Requisitos de negócio para controle de acesso

A-11.2 Gerenc.de Acessos de Usuário

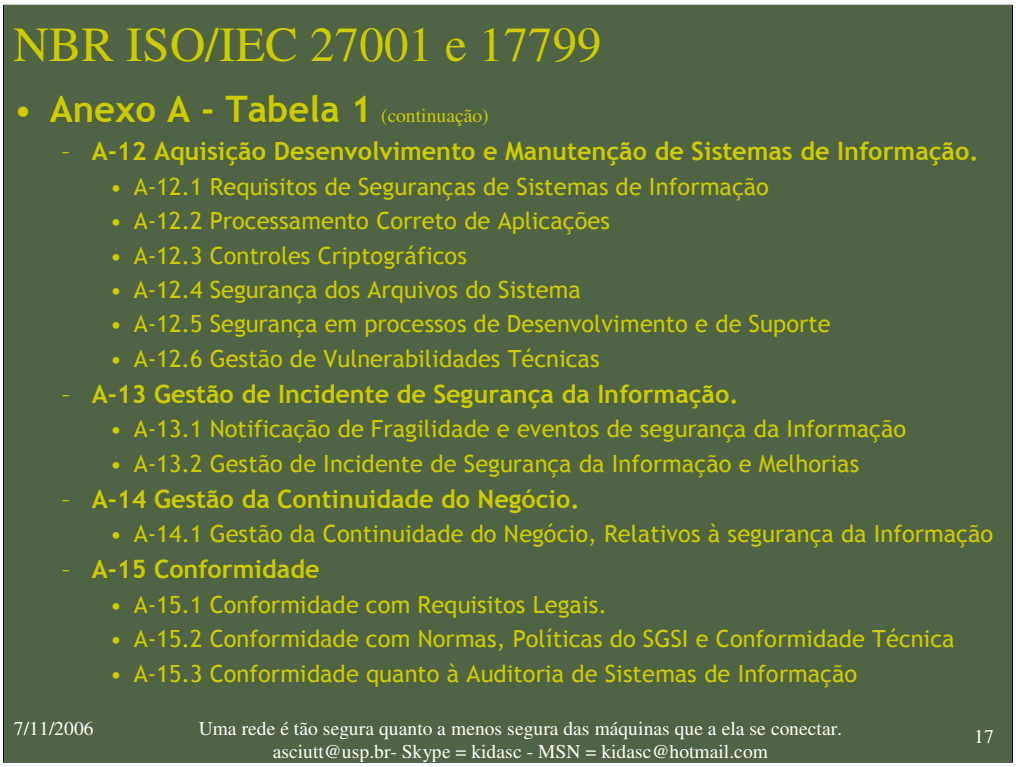
A-11.3 Responsabilidades dos Usuários

A-11.4 Controle de acessos a rede

A-11.5 Controle de acesso ao Sistema Operacional

A-11.6 Controle de acesso à aplicativos e à informação

A-11.7 Computação Móvel e Trab.Remoto



Anexo A

Tabela 1

.....

A-12 Aquisição Desenvolvimento e Manutenção de Sistemas de Informação.

A-12.1 Requisitos de Seguranças de Sistemas de Informação

A-12.2 Processamento Correto de Aplicações

A-12.3 Controles Criptográficos

A-12.4 Segurança dos Arquivos do Sistema

A-12.5 Segurança em processos de Desenvolvimento e de Suporte

A-12.6 Gestão de Vulnerabilidades Técnicas

A-13 Gestão de Incidente de Segurança da Informação.

A-13.1 Notificação de Fragilidade e eventos de segurança da Informação

A-13.2 Gestão de Incidente de Segurança da Informação e Melhorias

-14 Gestão da Continuidade do Negócio.

A-14.1 Gestão da Continuidade do Negócio, Relativos à segurança da Informação

A-15 Conformidade

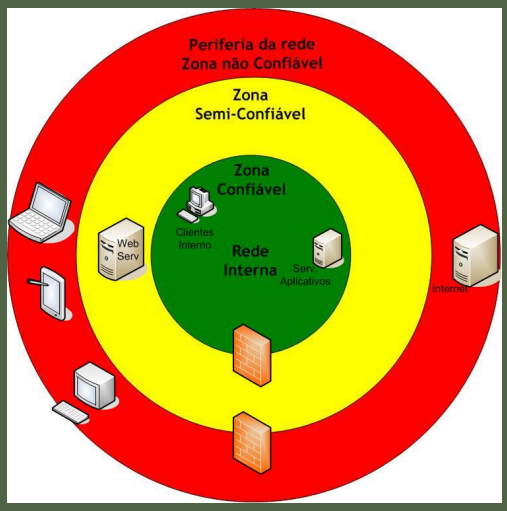
A-15.1 Conformidade com Requisitos Legais.

A-15.2 Conformidade com Normas, Políticas do SGSI e Conformidade Técnica

A-15.3 Conformidade quanto à Auditoria de Sistemas de Informação

Defesas em Rede:

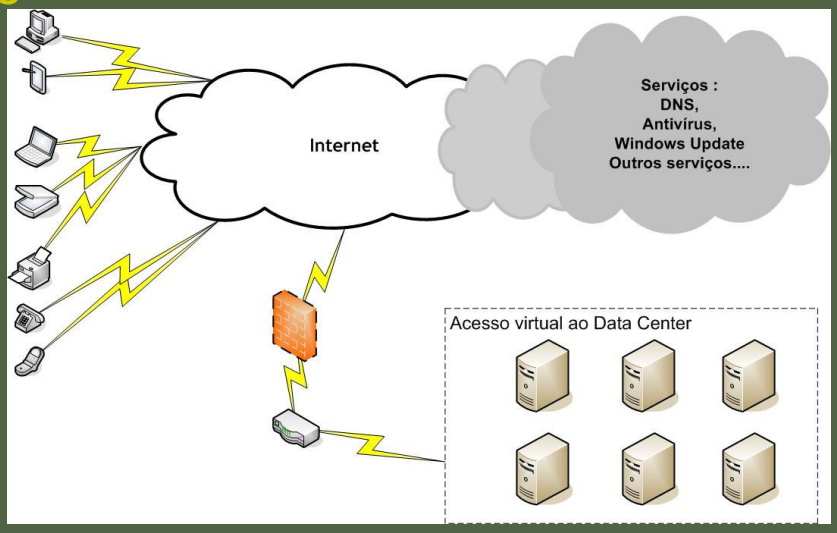
- **Anterior:**



Segurança por zona em três camadas, ISSA Journal, abril 2006

Defesas em Rede:

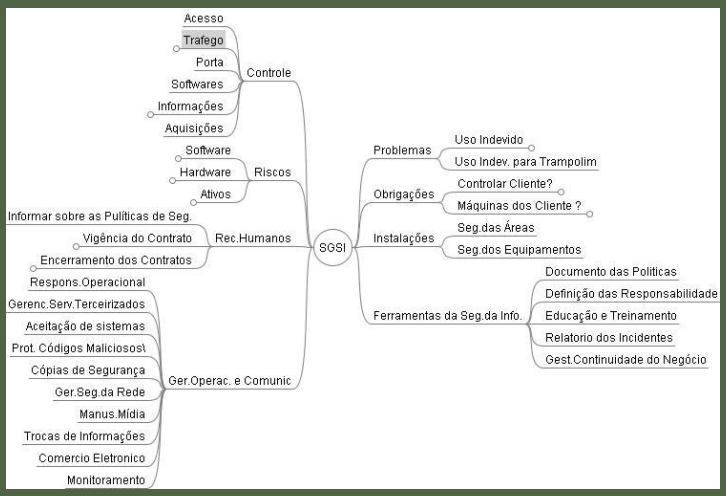
- **Sugerida Atualmente:**



Nova Arquitetura de segurança, usuários com acesso por rede ao Virtual Data Center. ISSA Journal, abril

Proposta de Plano de Trabalho/Ação

- Proposta de Trabalho Mapa Conceitual e Segurança da Informação
- Ajuste do mapa pela NBR ISO/IEC-17799-2005 e NBR ISO/IEC-27001-2006



Mapa conceitual de segurança (reduzido).

7/11/2006 Uma rede é tão segura quanto a menos segura das máquinas que a ela se conectar. asciutt@usp.br- Skype = kidasc - MSN = kidasc@hotmail.com 20

Mostrar como foi a construção do mapa.

Do Centro para fora.

Mostrar que ele é maior que o apresentado,

Mostrar como funciona,

Ficar visível

Colorir os nós, identificando etapas, implantado, planejado, etapas fases.

Proposta de Plano de Trabalho/Ação

- **Planejamento e Ações :**
- o Mapear a área de atuação:
  - o Levantamento completo do SGSI.
- o Planejar Etapas de implantação:
  - o Seguimentar o Mapa de Atuação, "Não ser mais realista que o Rei".
- o Criação da Brigada de Segurança da Informação:
  - o Pulverizar e Conscientizar as práticas de segurança da Informação.
- o Divulgar.
  - o Documentos padrão de divulgação e locais de avisos.
- o Treinar.
  - o Planejar os treinamentos para todos os níveis e todos os envolvidos, Doscentes, Discentes, Funcionários.

Obrigado

Referencia :

- NBRISO/IEC27001 de 03/2006
- NBRISO/IEC17799 de 2001
- ISSA – Journal (Information System Security Association)

Links sobre segurança Pró-Ativa:

- Ponemon ONG sobre segurança da informação. http://www.ponemon.org/
- Modulo Security. http://www.modulo.com.br
- Sopho. http://www.sophos.com/
- Linux Security. http://www.linuxsecurity.com/
- Organisation for Economic Co-operation and Development
  http://www.oecd.org/home/0,2987,en_2649_201185_1_1_1_1_1,00.html

César Augusto Asciutti
Agência USP de Inovação
asciutti@usp.br
Fone – 3091-2933
Skype – kidasc - MSN – kidasc@hotmail.com

Uma rede é tão segura quanto a menos segura das máquinas que a ela se conectar.
asciutt@usp.br- Skype = kidasc - MSN = kidasc@hotmail.com