



ISO/IEC 17799 - 27001

Clauzio
Cleber
Hugo Azevedo
Roger

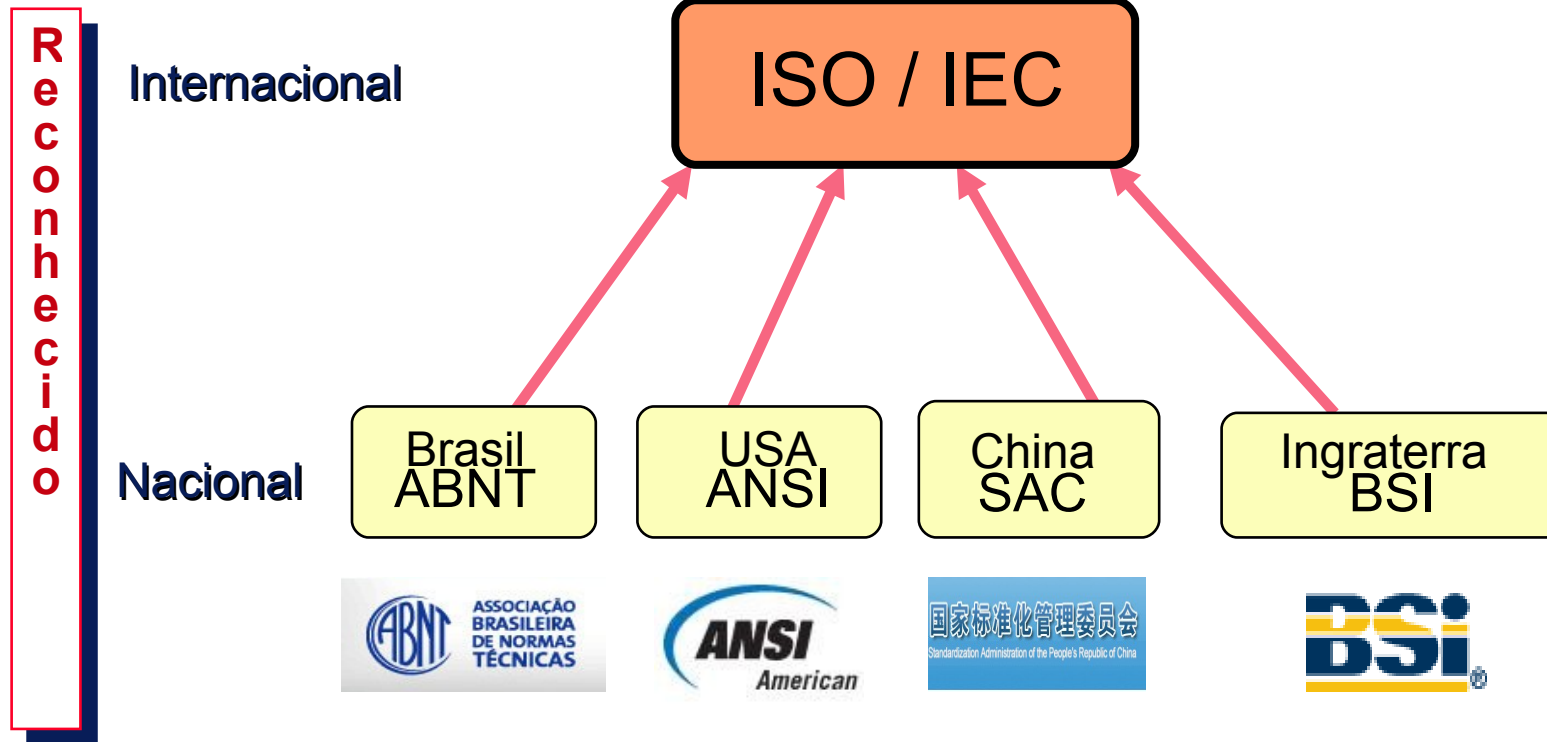


ISO/IEC 17799 - 27001



- ISO: Organização de Padronização Internacional:
 - ISO 9001 e 14001;
- IEC: Comissão Eletrotécnica Internacional:
 - IEC 60950-1 (ITE: Safety);
- ISO/IEC: Cooperação entre ISO e IEC;
 - Para não evitar o **OVERLAP** de padrões;

Estrutura dos Orgãos de Padronizações





ISO/IEC 17799 - 27001



Tudo começou ...

- **BS 7799;**
- BSI (British Standards Institute);
- Organização Inglesa de Padronização;
- BS 7799-1, BS 7799-2 e BS 7799-3;





BS 7799-1

- 1995;
- Códigos de Boas Práticas para o Gerenciamento da Segurança da Informação;



BS 7799-2

- 1999;
- Sistema de Gerenciamento da Segurança da Informação;



BS 7799-3

- 2005;
- Análise e Gerenciamento de Riscos;



ISO/IEC



- Outros países adotaram a **BS 7799**;
- ISO/IEC;
- Em 2000;
- **ISO/IEC 17799** que foi baseada na BS 7799 parte 1;
- Revisada em 2005;



As séries 27000



- ISO/IEC 27000, 27001, 27002, 27003, 27004, 27005, 27006, 27007, ... , 27799;
- Onde algumas foram baseadas nas BS 7799 e na ISO 17799;



Tabela Evolutiva



BSI	ISO/IEC	ISO/IEC	Objetivo	Lançamento
		ISO 27000	Vocabulário	Em preparação
BS7799-2		ISO 27001	SGSI	2005
BS7799-1	ISO 17799	ISO 27002	Cód. Boas Práticas	Previsão p/ 2007
		ISO 27003	Nova SGSI	Em preparação
		ISO 27004	Medições	Em preparação
BS7799-3		ISO 27005	Gerenciar Riscos	Previsão p/ 2007
		ISO 27006	Guia p/ Certificação	2007
		ISO 27007	Guia de Auditoria	Em preparação
...
		ISO/DIS27799	Cuidados Indústrias	Em preparação



Escopo do Trabalho



- ISO/IEC 17799;
- ISO/IEC 27001;



ISO/IEC 17799



Código de Prática para a Gestão da Segurança da Informação

- Definições (17)
 - ativo, controle, diretriz, recursos de processamento da informação, segurança da informação, evento de segurança da informação, incidente de segurança da informação, política, risco, análise de riscos, análise/avaliação de riscos, avaliação de riscos, gestão de riscos, tratamento do risco, terceira parte, ameaça, vulnerabilidade



ISO/IEC 17799



Código de Prática para a Gestão da Segurança da Informação

• Algumas definições (17)

- ativo
 - qualquer coisa que tenha valor para a organização
- controle
 - forma de gerenciar o risco, incluindo políticas, procedimentos, diretrizes, práticas ou estruturas organizacionais, que podem ser de natureza administrativa, técnica, de gestão ou contramedida.
- segurança da informação
 - preservação da confidencialidade, da integridade e da disponibilidade da informação
- política
 - intenções e diretrizes globais formalmente expressas pela direção



ISO/IEC 17799



Objetivo

- Estabelecer códigos de boas práticas para a gestão de segurança da informação
- Dar instrumentos para a implantação de segurança da informação de acordo com a características de uma empresa



ISO/IEC 17799

Seções



- a) Política de Segurança da Informação (1);
- b) Organização a Segurança da Informação (2);
- c) Gestão de Ativos (2);
- d) Segurança em Recursos Humanos (3);
- e) Segurança Física e do Ambientes (2);
- f) Gestão das Operações de Comunicação (10);
- g) Controle de Acesso (7);
- h) Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação (6);
- i) Gestão de Incidentes de Segurança da Informação (2);
- j) Gestão da Continuidade do Negócio (1);
- k) Conformidade (3).



ISO/IEC 17799

Principais Categorias



Cada categoria principal de Segurança da Informação contém:

- a) um objetivo de controle que define o que deve ser alcançado; e
- b) um ou mais controles que podem ser aplicados para se alcançar o objetivo do controle



ISO/IEC 17799

Estrutura dos Controles



- Controle
 - definição do controle
- Diretrizes para a implementação
 - informações mais detalhadas
- Informações adicionais
 - considerações legais e referências a outras normas



ISO/IEC 17799

Política de Segurança



- A política de segurança é um conjunto de normas e diretrizes destinadas a proteção dos ativos da Organização;
- Prover à administração uma direção para Segurança da Informação;
- Convém que a Política seja clara, flexível e aprovada pela administração, publicada e comunicada, de forma oficial, para todos os funcionários e partes externa relevantes;



ISO/IEC 17799

Política de Segurança



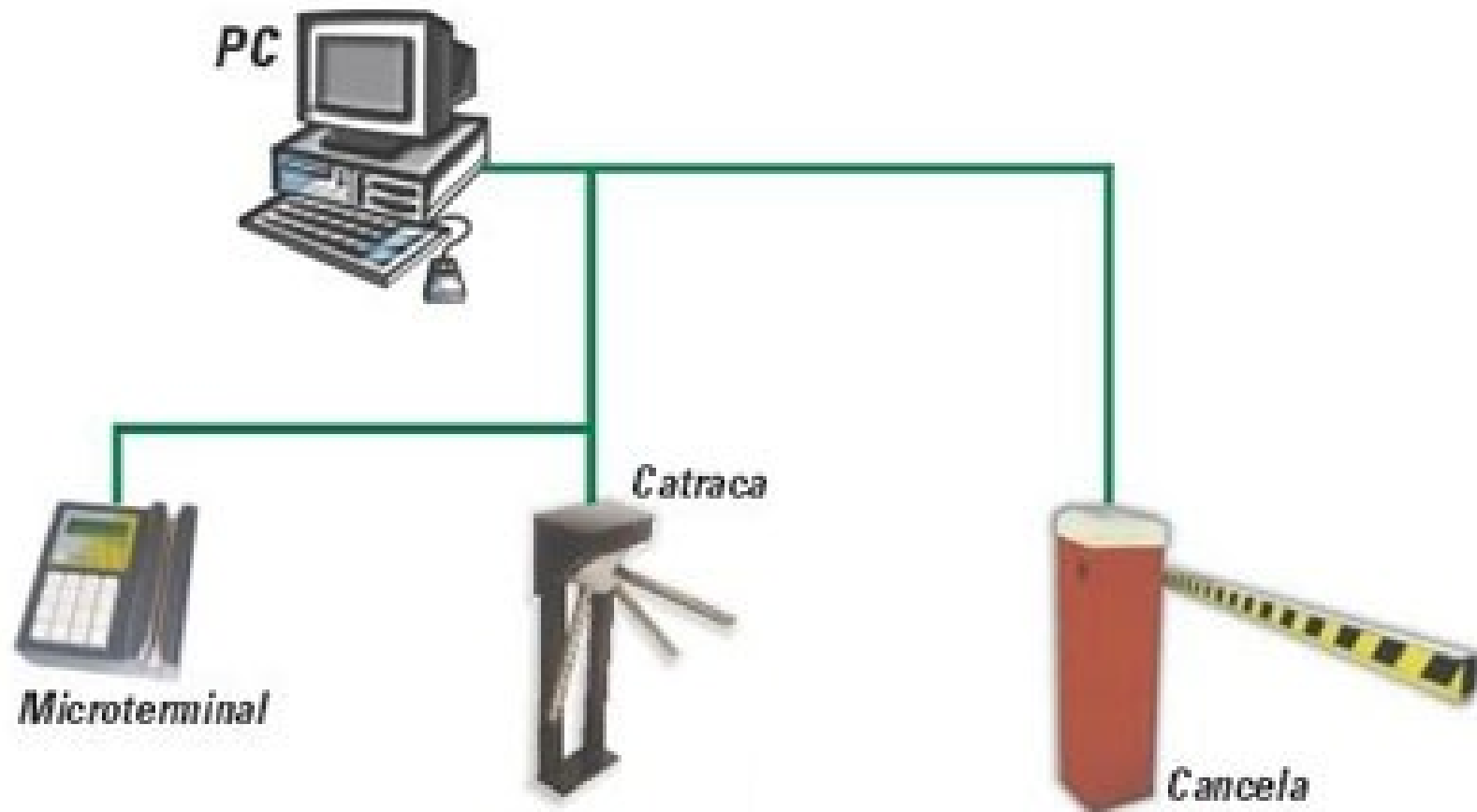
- Definições das reponsabilidades na gestão de segurança;
- Referências à documentação que possam apoiar a política;

Controles

- Controles de entrada física;
- Controles contra códigos maliciosos e móveis;
- Controles de acesso ao SO e a rede;
- Controles criptográficos;

Controles

- Controles de entrada física;



Controles

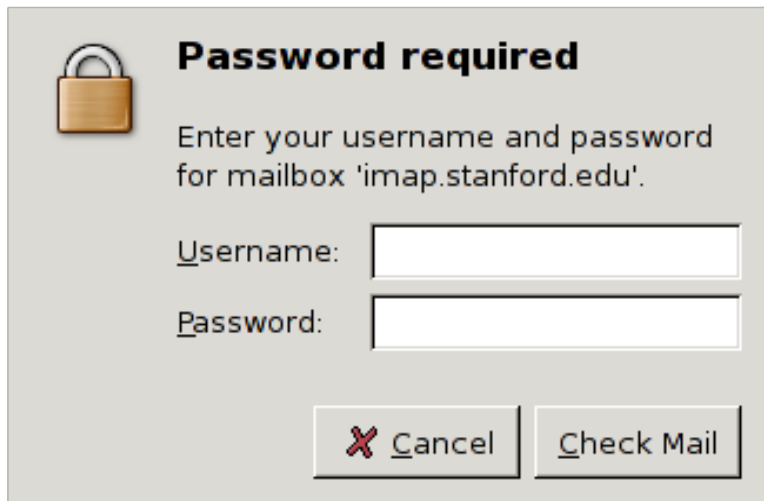
- Controles contra códigos maliciosos e móveis;




Controles

- Controles de acesso ao SO e a rede;

```
hugo@amd2800:~$ su
Password: █
```



 **Password required**

Enter your username and password for mailbox 'imap.stanford.edu'.

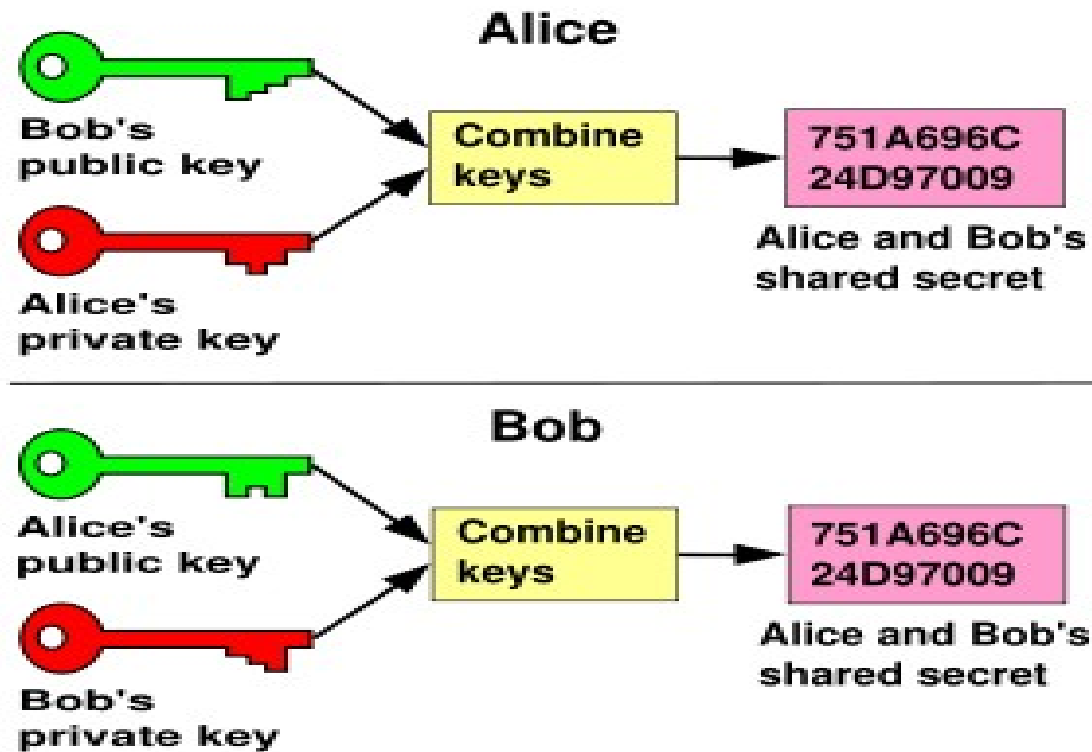
Username:

Password:



Controles

- Controles criptográficos;





ISO 27001



- O padrão de certificação
 - Baseada na BS 7799-2002 Parte 2
 - Alinhada com ISO 9001 e 14001 (compatível)
- Objetivos
 - Atender todos os tipos de organizações
 - Prover modelo para estabelecer, implementar, ..., e melhorar um SGSI

- “Importância da Segurança Informação”
 - Quanto custará uma falha que implique na perda efetiva de informação ?
 - Quais as consequências da utilização de informação por pessoas que dela possam fazer uso indevido e não autorizado ?
 - Qual o custo da diminuição de produtividade por erros, falhas de sistema ou utilização de informação errada ?
 - Você está preparado para o próximo incidente com a sua informação ?

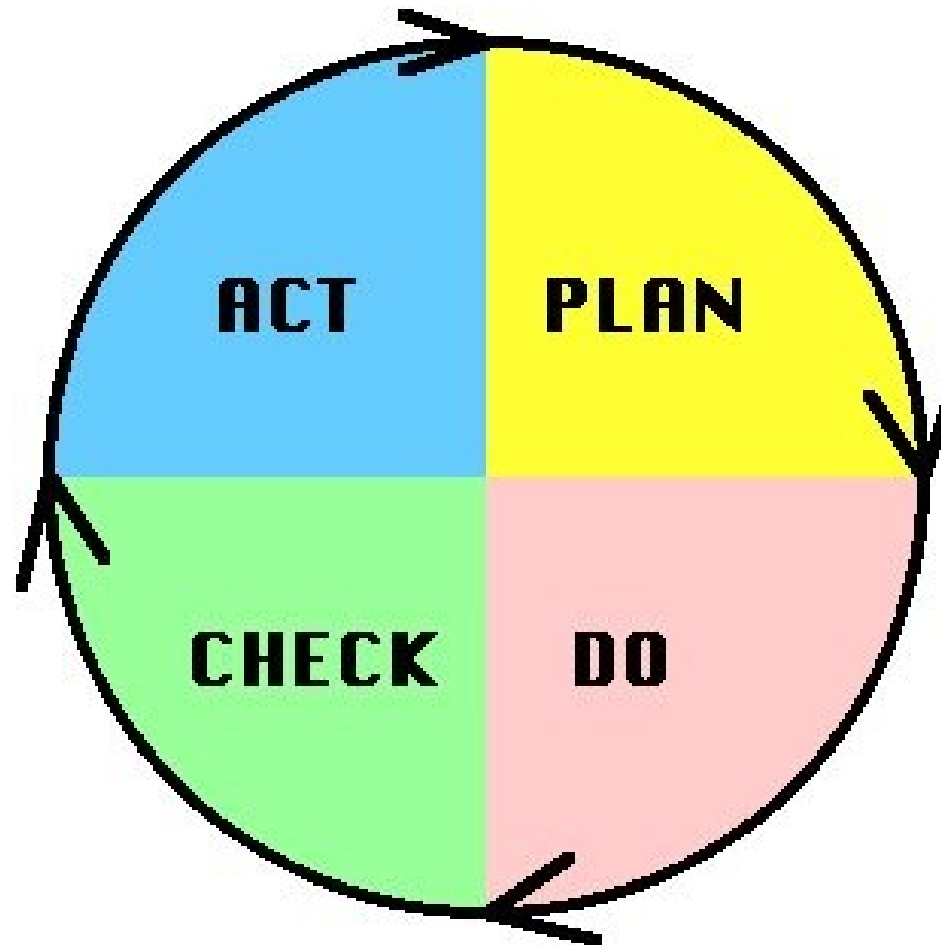


ISO 27001



- Requisitos
 - Todas as atividades devem seguir um processo (PDCA)
 - Objetivos de segurança precisam ser especificados
 - Controles devem ser baseados na análise de risco
 - Verificação e melhoria do processo devem ser contínuas

- FLUXO DO PDCA





ISO 27001



- Componentes da ISO 27001
 4. Sistema de gestão de segurança da informação (SGSI)
 5. Responsabilidade da direção
 6. Auditorias internas
 7. Análise crítica do SGSI pela direção
 8. Melhoria do SGI



ISO 27001



- SGSI
 - Estabelecer o SGSI
 - Implementar e operar o SGSI
 - Monitorar e analisar criticamente o SGSI
 - Manter e melhorar o SGSI
 - Requisitos de documentação
 - Controle de Documentos
 - Controle de registros



ISO 27001



- Responsabilidade da direção
 - Comprometimento da direção
 - Gestão de Recursos
 - Provisão de recursos
 - Treinamento, conscientização e competência



ISO 27001



- Auditorias internas do SGSI
 - Auditorias internas do SGSI em intervalos planejados para determinar se SGSI:
 - atende requisitos da norma
 - atendem aos requisitos de segurança identificados
 - esta sendo executado conforme esperado
 - Procedimento documentado (responsabilidades, requisitos para planejamento e execução da auditoria)
 - Os auditores não devem auditar seu próprio trabalho (objetividade e imparcialidade)



ISO 27001



- Análise crítica do SGSI pela Direção
 - Analise do SGSI em intervalos planejados
 - Entradas: resultado de auditorias e análises críticas, situação das ações preventivas e corretivas, vulnerabilidades não contempladas adequadamente nas análises anteriores, resultados, recomendações, mudanças.
 - Saída: oportunidade de incluir melhorias e mudanças, modificação do SGSI (requisito de negócio), necessidade de recursos, etc...



ISO 27001



- Melhoria do SGSI
 - Melhoria contínua por meio do uso da política estabelecida, resultados das auditorias, análise dos eventos monitorados, ações corretivas (etapas anteriores)
 - Eliminação das não conformidades através de ações corretivas ou preventivas



ISO 27001



- Benefícios da certificação
 - Certificar que as melhores praticas estão sendo seguidas
 - Requisitos Governamentais
 - Diferencial de Marketing
 - Resultado natural de uma necessidade intrínseca dos tempos (terrorismo rsrsrs)



ISO 27001



- Empresas Certificadas
 - No Brasil apenas 15 organizações possuem certificado BS7799-2, dentre elas: Serasa, Banco Matone, Samarco, Modulo Security, Unisys, PRODESP, SERPRO, Telefonica.
 - Modulo Security foi a primeira empresa do mundo a obter certificação ISO 27001



Ferramenta

http://www.axlr.com.br - Portal - Information Security Management System - Microsoft Internet Explorer

ISMS Information Security Management System

AXLR INFORMATION SECURITY

Resumo: Tabela Resumo

Ultima Atualizacao: 21 de Maio de 2009, às 16:11 (por: 100.175.209.4)

De acordo com seu perfil, você poderá visualizar alguns relatórios. [Verifique suas preferencias.](#)

Sumário de Atividades

Atividade	Atividade	Atividade	Atividade	Atividade
Atividade (Resumo)	10	0	0	10
Processo (Resumo)	10	0	0	10
Atividade (Resumo)	0	0	0	0
Atividade (Resumo)	10	0	0	0
Atividade (Resumo)	10	0	0	0

Tarefas

ID Tarefa	Atividade	Atividade
10004/0004 10:00	Monitorar Situação Geral	0
10004/0004 17:00	Aprovar Ativa	0
10004/0004 18:00	Aprovar Ativa	0
10004/0004 18:00	Aprovar Ativa	0
10004/0004 18:00	Aprovar Ativa	0
10004/0004 18:00	Aprovar Ativa	0

Sumário de Controles


Controle	Controle	Controle
0/1	0/4	0/1

Atividades

ID Atividade	Atividade	Atividade
10004/0004 10:00	At implementação de atividades Real do Controle "Registros de Incidentes" sendo desativado.	0
10004/0004 10:00	At Controle "Registros de Incidentes" não está implementado.	0
10004/0004 10:00	At implementação de atividades Real do Controle "Registros de Incidentes" sendo.	0
10004/0004 10:00	At implementação de atividades Real do Controle "Registros de Incidentes" sendo desativado.	0
10004/0004 18:00	Ativa "Ativa" com uma implementação parcial de implementação de atividades de informações - Sistema de Proteção de Informações.	0

Gráficos

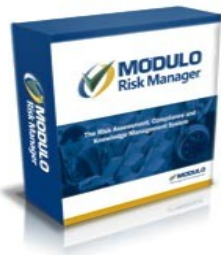
Atividade (Resumo)



Categoria	Valor
Atividade Ativa	10
Atividade Inativa	0
Atividade Total	10

AXLR | SOLUÇÕES PARA O SEU NEGÓCIO | INFORMAÇÃO SECURITY MANAGEMENT SYSTEM | MICROSOFT INTERNET EXPLORER

Concluído



Ferramenta



Modulo Risk Manager - Risk Analysis Report

Project: Risk Analysis

Scope: All

Asset Type: All

Business Compon: All

Checklist: All

Generate

Save

Open Document in MS Word

RISK ANALYSIS REPORT

2. MAIN CONCLUSIONS

2.1. Decision-Making Indexes

The Decision-Making Index is a tool to assist management in prioritizing corrective actions and implementations. The indicators used are:

Compliance Index (Compliance Indicator) - This index is calculated by dividing the total amount of controls that have been implemented by the total amount of applicable controls. This score can range from 0% to 100%.

Security Index (Security Indicator) - This index is calculated by dividing the total of risks of the controls that have been implemented (Avoided PSR) by the total of risks of the applicable controls (Total PSR). This index can range from 0% to 100%.

PSR (Absolute Risk number) - This number is the sum of the results of the PSR of the controls that have not been implemented.

Applicable Controls (926)		Applicable Risks (39880)	
Implemented Controls (421) - 45.48%	Non-Implemented Controls (505) - 54.54%	Avoided Risks (18042) - 45.24%	Existing Risks (21838) - 54.76%

Compliance Index (Quantitative view)

The following chart shows that from a total of 926 applicable controls in the analysis, there are 505 controls that have not been implemented (54.54%). Thus, the result of the Compliance Index was 45.48%. It must be understood that the higher the Compliance Index, the more in conformity with the base of the used checklists the results are. As it can be seen in previous table, the Non-Compliance Index found was 54.54%.

Per Controls

CONCLUSÃO

ALGUÉM SE ABILITA?

Referências Bibliográficas

- ISO/IEC 17799
- ISO/IEC 27001
- <http://www.iso.org>
- <http://www.iec.ch/>
- http://en.wikipedia.org/wiki/ISO_27001
- http://en.wikipedia.org/wiki/ISO_17799
- <http://www.modulo.com.br/>
- <http://www.axur.com.br/>