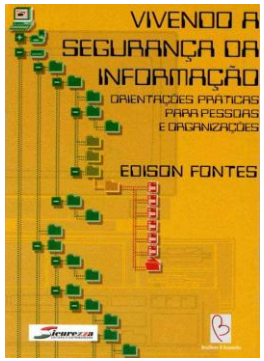
Praticando a Segurança da Informação

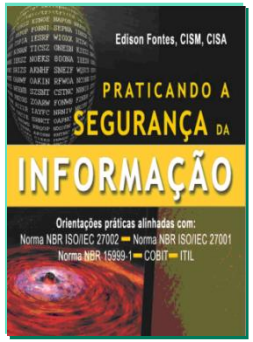
Edison Fontes, CISM, CISA

edison@pobox.com

NÚCLEO
CONSULTORIA EM SEGURANÇA

Cabo Verde, Praia, 03 de Dezembro de 2010





Segurança da Informação desde 1989

- *Coordenador Banco BANORTE*
- *Gerente de PricewaterhouseCoopers*
- *Security Officer da GTECH Brasil*
- *Executivo da Prática Segurança Informação – CPM Braxis*
- *Núcleo Consultoria em Segurança.*

Livros

- *Praticando a segurança da informação, Editora Brasport, 2008.*
- *Por quê GESITI?, Editora Komedi, CENPRA/MCT, 2007, Co-autor.*
- *Segurança da Informação: o usuário faz a diferença, Editora Saraiva, 2005.*
- *Vivendo a Segurança da Informação, Editora Sicurezza, 2000.*
- *Banco Eletrônico, PwC, Edição FEBRABAN, 2000, Co-autor.*
- *"Guia Básico para Projetos de Segurança Lógica de Dados" – FEBRABAN, 1991, Co-autor.*
- *Innovations and Advanced Techniques in Computer and Information Sciences and Engineering, Springer/USA, 2007, Co-Autor.*

Colunista

- *Portal ITWEB www.itweb.com.br*

Ativos da Organização

- **Ativos Tangíveis**
- **Ativos Intangíveis**
  - Ativos intangíveis que **Geram valor**
  - Ativos intangíveis que **Protegem valor**

Fonte: Livro Ativos Intangíveis

Daniel Domeneguetti, Roberto Meir

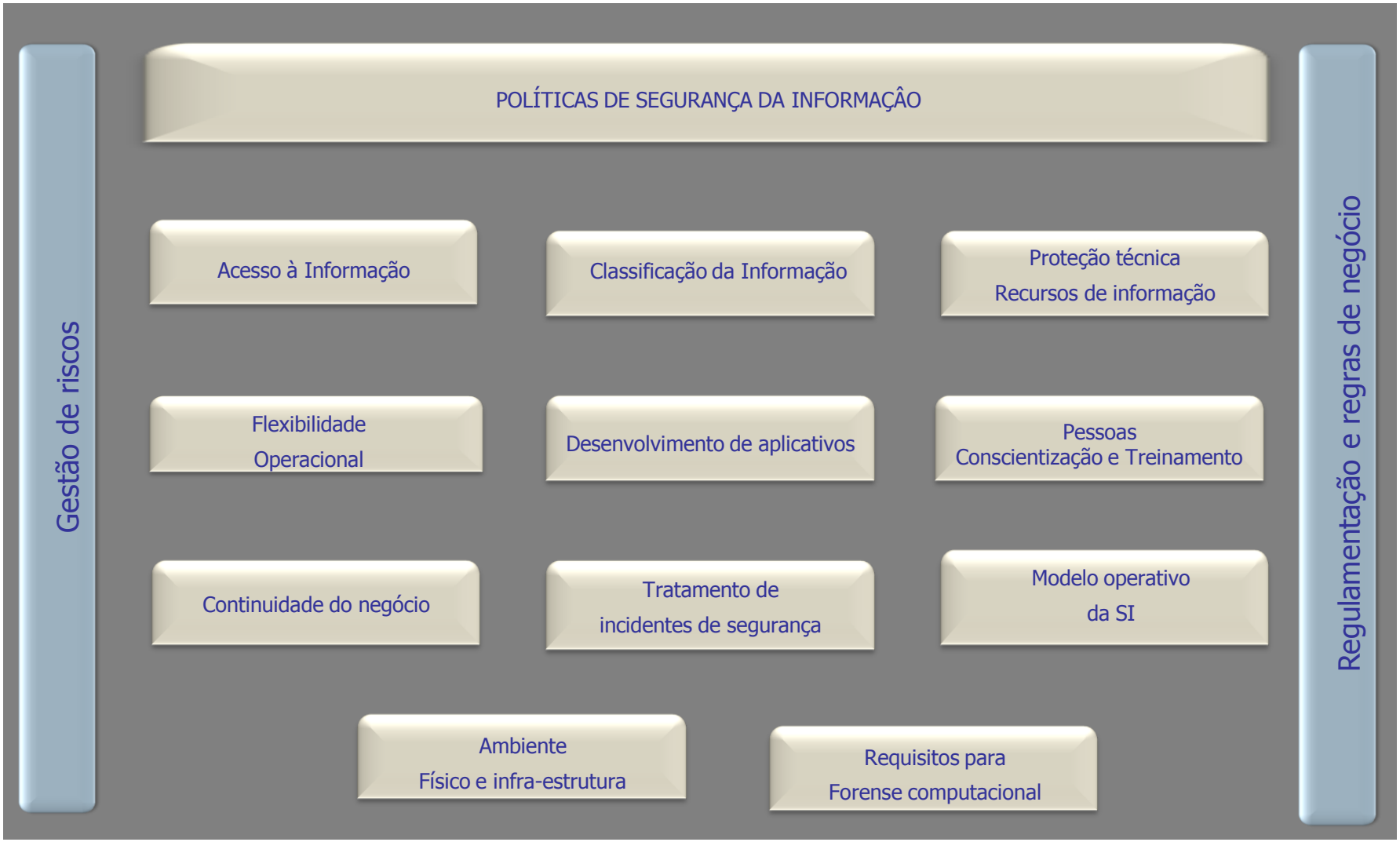
Editora Campos, Brasil, 2008

Ambiente da Informação

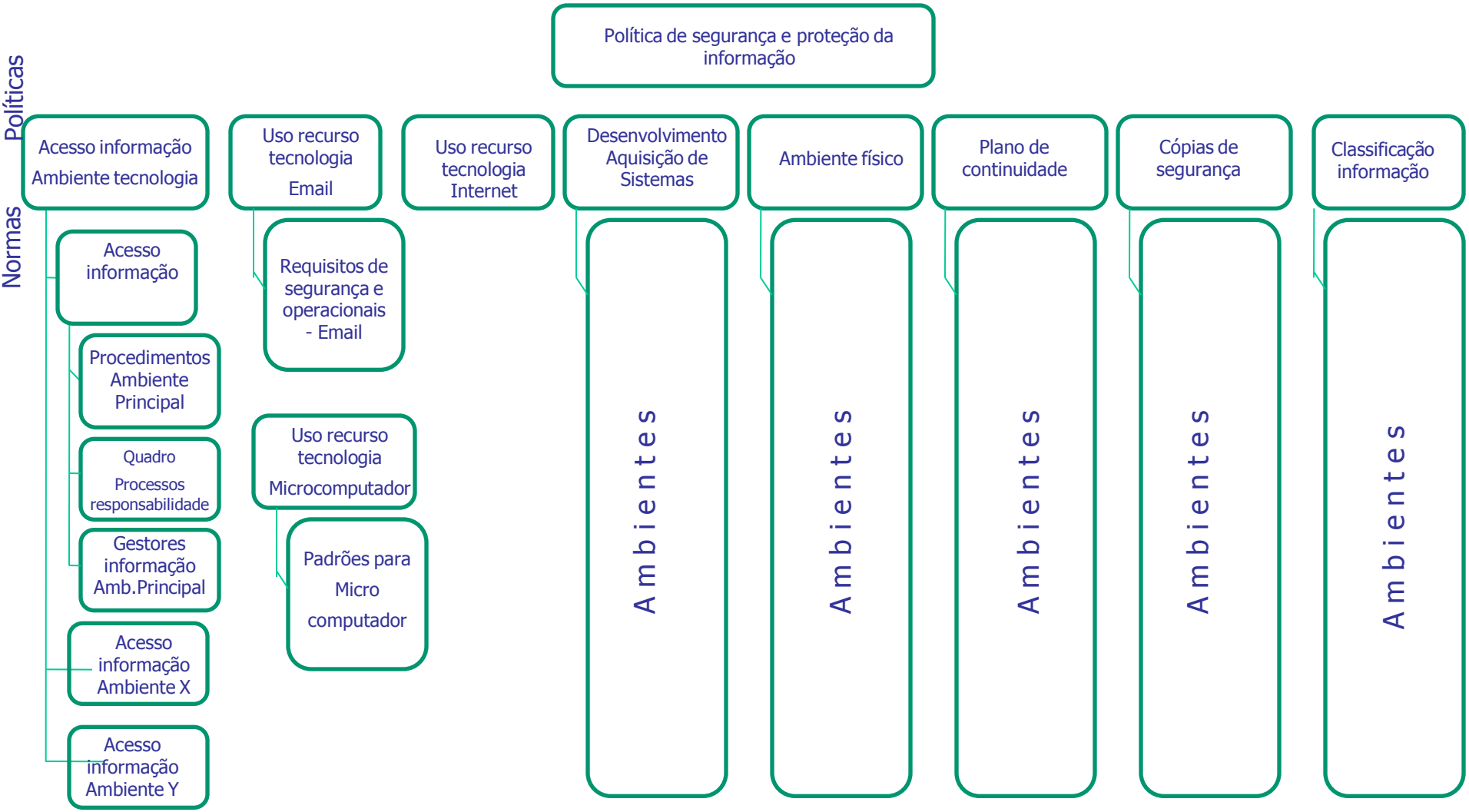
Contingências

Crime organizado

Processo Corporativo de Segurança da Informação



Estrutura proposta para as Políticas e Normas



Segurança da Informação

Acesso à Informação

Identificação

- Identidade usuário
- Ciclo de vida da identidade
  - Criação
  - Bloqueio
  - Retirada
  - Outras ações

Gestão de Identidade

Autenticação

- Verificação da veracidade do usuário
- Utilização de senha, biometria, *tokens*

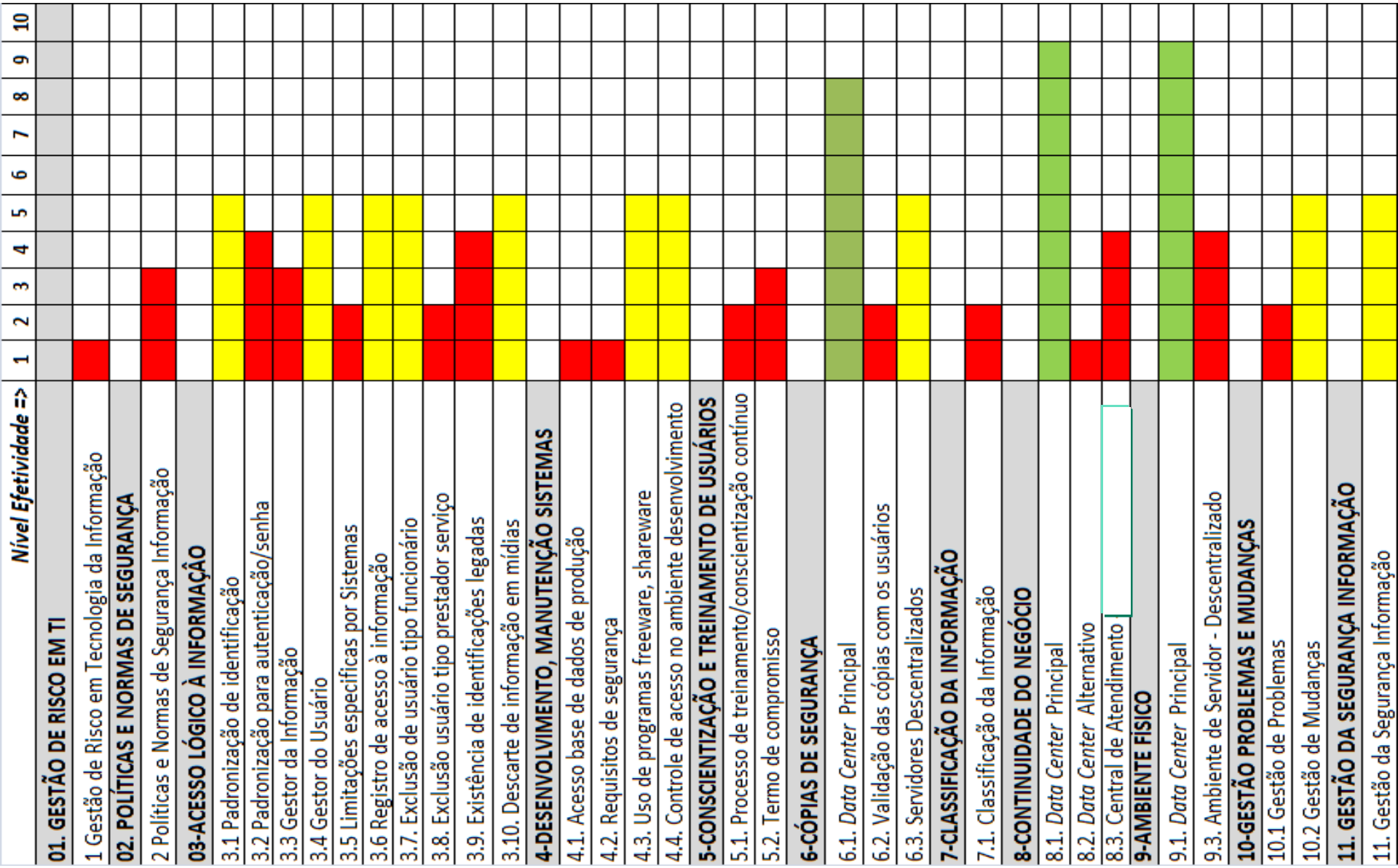
Gestão de Autenticação

Autorização

- Verificação se usuário está autorizado
- Acesso ao recurso
- Modelo de autorização (perfil, unitário, grupo)

Gestão de Autorização

Avaliação da Gestão da Segurança da Informação



Planejamento para a Gestão da Segurança da Informação

AMEAÇAS / VULNERABILIDADES	Solução Proposta	OK em													Observações
01-GESTÃO DE RISCO EM TI			3	6	9	12	15	18	21	24	27	30	33	36	
1- Gestão de Risco em Tecnologia da Informação	Implantar Gestão de Risco SI	6 meses			X	X									
02.REGULAMENTOS DE SEGURANÇA (Politicas, Normas)															
2.1 Políticas e Normas de Segurança Informação	Política principal+ N2+Acesso (N3)	6 meses	X	X											Estrutural
	Demais regulamentos	12 meses			X	X									Estrutural
03-ACESSO LÓGICO À INFORMAÇÃO															
3.1-Padronização de identificação	Garantir o uso do padrão	6 meses	X	X											
3.2-Padronização para autenticação/senha	Definir e padronizar regras senha	6 meses	X	X											
	Iniciar em novos sistemas	6 meses	X	X											
	Alterar sistema atuais	12 meses	X	X	X	X									
3.3-Gestor da Informação	Implantar	12 meses	X	X	X	X									Estrutural
3.4-Gestor de Usuário	Implantar	6 meses	X	X											Estrutural
3.5-Limitações específicas por sistemas	Identificar e desenvolver solução	24 meses					X	X	X	X					
3.6-Registro de acesso à informação	Identificar situaçao dos sistemas	6 meses	X	X											
	Implantar requisitos de log acesso	12 meses			X	X									
3.7-Exclusão usuário tipo funcionário	Estruturar e garantir controle atual	6 meses	X	X											
	Solução mais integrada/automática	18 meses			X	X	X	X							
3.8-Exclusão usuário tipo prestador de serviços	Criar controle manual/efetivo	6 meses	X	X											
	Solução mais integrada/automática	24 meses					X	X	X	X					
3.9-Existência de identificações legadas	Limpar diretorios e similares	12 meses	X	X	X	X									
3.10-Descarte de informação em mídias	Garantir cumprimento regulamento						X	X							
4-DESENVOLVIMENTO, MANUTENÇÃO SISTEMAS			3	6	9	12	15	18	21	24	27	30	33	36	
4.1-Acesso a base de dados de produção	Definir e implantar controles	24 meses	X	X	X	X	X	X	X	X					
4.2-Requisitos de segurança	Implantar no proc. desenv.sistemas	6 meses	X	X											Estrutural
4.3-Uso de programas freeware e shareware	Definir regras + implantar	6 meses	X	X											
4.4-Controle de acesso no ambiente de desenvolvimento	Manter e melhorar controles	12 meses													
5-CONSCIENTIZAÇÃO E TREINAMENTO DE USUÁRIOS															
5.1-Processo de treinamento/conscientização contínuo	Implementar consc./treinamento	36 meses	X	X	X	X	X	X	X	X	X	X	X	X	Estrutural
5.2-Termo de compromisso	Elaborar Termo Confidenc.	6 meses	X	X											Estrutural
6-CÓPIAS DE SEGURANÇA															
6.1-*Data Center* Principal	Garantir nível atual-Def. controles	6 meses	X	X											
6.2-Validação das cópias com os usuários	Realizar validação com usuários	12 meses			X	X									
6.3-Servidores Descentralizados	Garantir mudança para EDS 12.2009	6 meses	X	X											
7-CLASSIFICAÇÃO DA INFORMAÇÃO															
7-Classificação da Informação	Definir níveis de sigilo	6 meses	X	X											
	Implantar no ambiente Medial	36 meses			X	X	X	X	X	X	X	X	X	X	
8-CONTINUIDADE DO NEGÓCIO															
8.1-*Data Center* Principal	Garantir nível atual-Definir controles	6 meses	X	X											
8.2. *Data Center* Alternativo	Implementar solução	12 meses			X	X									
8.3-Central de Atendimento TelePerformance	Contratar opção 2o. Local	12 meses			X	X									
9-AMBIENTE FÍSICO			3	6	9	12	15	18	21	24	27	30	33	36	
9.1-*Data Center* Principal	Garantir nível atual-Definir Controles	6 meses	X	X											
9.2-Ambiente de Servidor Descentralizado	Garantir mudança para EDS 12.2009	6 meses	X	X											
10-GESTÃO DE PROBLEMAS, MUDANÇAS E INCIDENTES															
10.1-Gestão de Mudanças	Consolidar Gestão Mudanças	6 meses	X	X											Estrutural
10.2-Gestão de Problemas	Implantar Gestão Problemas	12 meses			X	X									Estrutural
11-GESTÃO DA SEGURANÇA DA INFORMAÇÃO															
11.1-Gestão da Segurança da Informação	Aprimorar a Gestão da Segurança	36 meses	X	X	X	X	X	X	X	X	X	X	X	X	Estrutural

Segurança da Informação – Exigencias (Futuras)

- Novas, novas, novas tecnologias.
- Redes sociais (pessoas, organizações, governo).
- Maior Mobilidade.
- Maior quantidade de informação. Conhecimento (???).
- Maior busca pela privacidade.
- Maior quantidade de informação em um único lugar – maior facilidade de vazamento.

O que fazer?

- *Ter regulamentos claros (Qual proteção se quer?)*
- *Investir nas pessoas*
- *Ter alinhamento com os objetivos da organização*
- *Planejar a segurança da informação*
- *Executar a segurança da informação*

Alinhamento aos objetivos da Organização

Área de Segurança da Informação

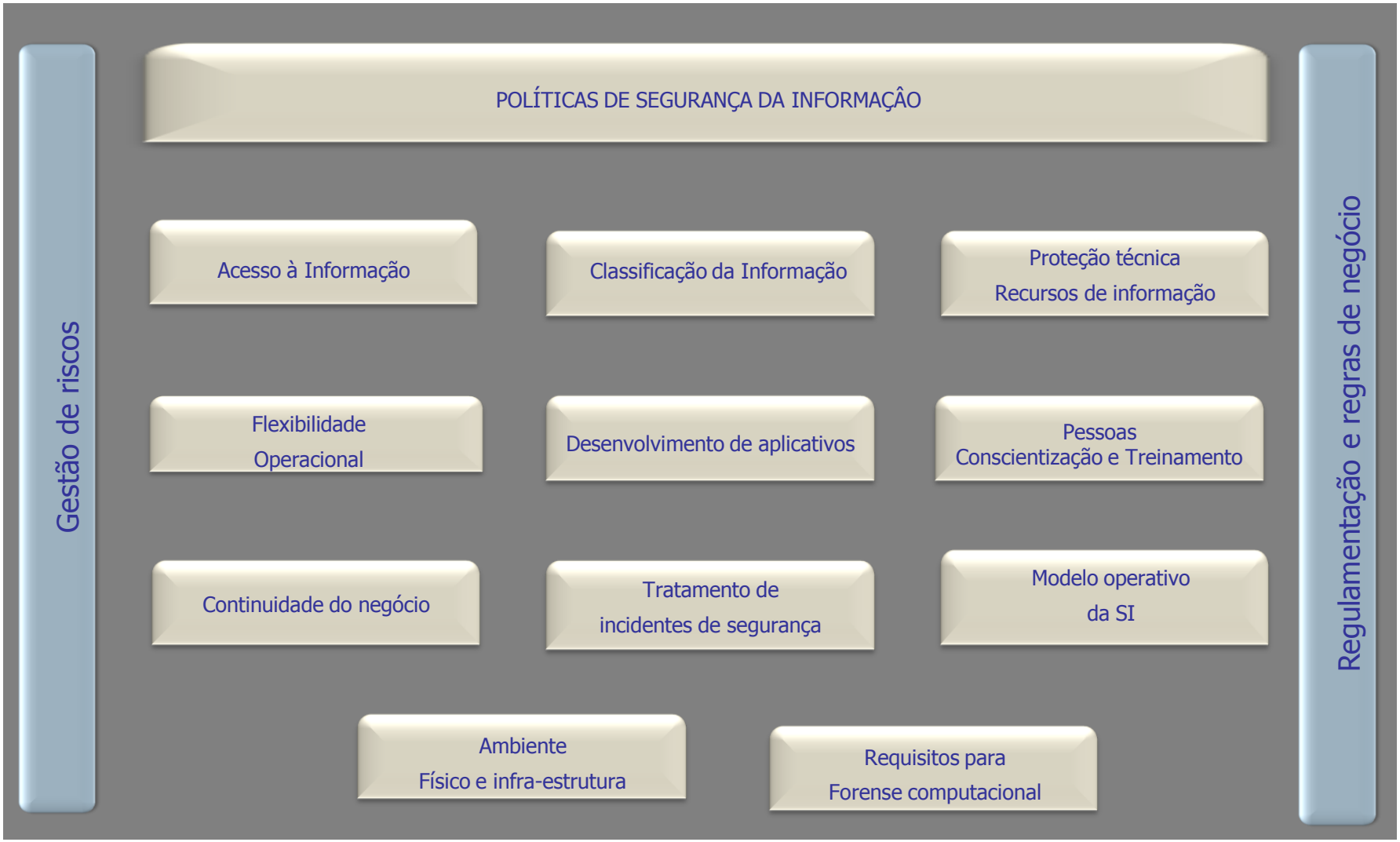
-Ter um nível hierárquico adequado.

- Conhecer a estratégia da Organização.

- Participar dos projetos deste o início.

- Os objetivos da Organização são a razão de ser da S.I.

Processo Corporativo de Segurança da Informação



Edison Fontes, CISM, CISA

edison@pobox.com

edison.fontes@uol.com.br

Cel. (55-11) 9132-5526

Link de artigos:

http://www.itweb.com.br/blogs/blog.asp?cod=58