AUDITORIA EM SISTEMAS E SEGURANÇA DA INFORMAÇÃO

Professor Me. Vladimir Geraseev Junior

ISO 27001 E POLITICA DE INFORMAÇÃO

O que é ISO?

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION

SEDE: Genebra – Suíça.
FUNDAÇÃO: 1946.
PAÍSES INTEGRANTES: 161.
BRASIL: ABNT – Associação Brasileira de Normas Técnicas.

O que é IEC?

INTERNATIONAL ELECTROTECHNICAL COMMISSION

FUNDAÇÃO: 1906.
OBJETIVO: Desenvolver e promover normas na área da tecnologia elétrica, incluindo eletrônica, eletroacústica, energia, etc.

Introdução:

AS NORMAS DA FAMÍLIA ISO 27000:

ISO/IEC 27000: Visão geral / introdução a família ISO 27000.

ISO/IEC 27001: é a norma que defini os requisitos para um Sistema de Gestão da Segurança da Informação (SGSI). É a principal norma que uma organização deve utilizar como base para obter a certificação empresarial em gestão de SI. É conhecida como a única norma auditavel que define os requisitos para um SGSI.

ISO 27001 foi baseado e substitui o BS7799.

Segurança da Informação.

-Normas traduzidas pela ABNT:

***NBR ISO/IEC 17799:2005 – Tecnologia da Informação – Técnicas De segurança – Código de Prática para Gestão de Seg. da Informação.**

-Controles da Segurança da Informação.

***NBR ISO/IEC 27002:2005 – Política de Segurança – Segurança em Recursos Humanos – Segurança física e do ambiente – Controle de acessos – Aquisição, desenvolvimento e manutenção de sistemas de informação – Gestão de Incidentes de Seg. da Informação – Gestão da continuidade do negócio – Conformidade.**

Segurança da Informação.

-Normas traduzidas pela ABNT:

***NBR ISO/IEC 27001:2006 – Tecnologia da Informação – Técnicas De segurança – Sistema de Gestão de Seg. da Informação - Requisitos.**

-Requisitos de sistemas de gestão da Informação.

***NBR ISO/IEC 27005:2008 – Tecnologia da informação – Técnicas de Segurança – Gestão de riscos de Seg. da Informação e manutenção de sistemas de informação.**

Segurança da Informação.

-Normas traduzidas pela ABNT:

***NBR ISO/IEC 27011:2009 – Tecnologia da Informação – Técnicas De segurança – Diretrizes para Gestão de Seg. da Informação para organizações de Telecomunicações baseadas na ABNT NBR ISO/IEC 27002: 2009.**

***NBR ISO/IEC 27004:2010 – Tecnologia da informação – Técnicas de Segurança – Gestão de Seg. da Informação – Medição.**

Onde aplicar a ISO 27000 e ISO 27001?

-Como metodologia estruturada com foco à segurança da informação.

-Como processo da segurança da informação (SGSI) para:

- Estabelecer;
- Implementar;
- Operar;
- Monitorar;
- Analisar criticamente;
- Manter;
- Melhorar um SGSI.

-Como controle, abrangendo as melhores práticas em SI.
-Aplica-se à empresas/organizações: independente do tamanho/ tipo/ natureza.

Onde aplicar a ISO 27000 e ISO 27001?

-Influências para especificação e implementação da SGSI.

- Necessidades e objetivos;
- Requisitos de segurança;
- Processos empregados;
- Tamanho e estrutura da organização.

-Espera-se que a SGSI seja aderente à evolução de seu:

- Ambiente;
- Sistema e
- Empresa.

-Espera-se usar a norma para avaliar a conformidade por partes:

- Internas. (ex: auditorias internas).
- Externas. (ex: empresas certificadoras).

Em que consiste?

-A norma padrão ISO 27001 foi baseado e substitui o BS 7799-2.

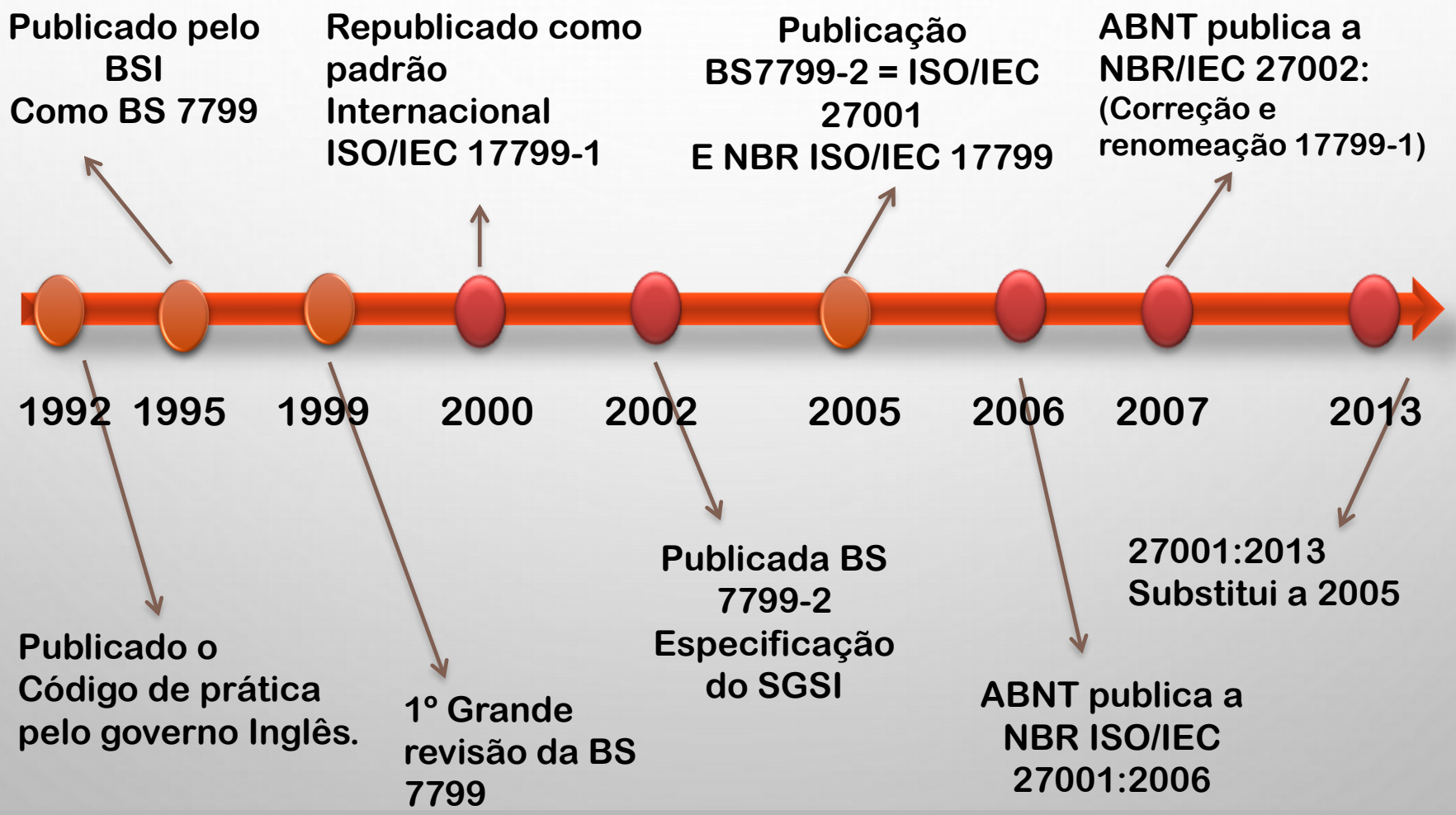
A norma ISO 27001 se originou da norma BS 7799, publicada pelo British Standards Institute (BSI). Revisada pela International Organization for Standardization (ISO), incorporou melhorias e adaptações, contemplando o ciclo PDCA de melhorias e a visão de processos que as normas de sistemas de gestão já incorporaram, como ISO 9001 (sistemas de gerência da qualidade) e ISO 14001 (sistemas de gerência ambiental).

Através de um trabalho em conjunto que veio sendo realizado desde 2000, a revisão foi feita por um comitê formado pela ISO e pelo International Electrotechnical Commission (IEC) onde as sugestões de alterações foram sendo compiladas, discutidas e apresentadas ao longo do trabalho.

Quais os benefícios?

1. Reduz o risco de responsabilidade por não implantação de um SGSI;
2. Identifica e corrige pontos fracos;
3. A alta direção assume a responsabilidade pela SI;
4. Permite revisão independente do SGSI;
5. Oferece confiança;
6. Melhor consciência sobre segurança;
7. Combina recursos com outros sistemas de gestão;
8. Mecanismo para medir o sucesso do sistema.

Breve histórico das normas:



Conceitos Básicos de SI:

-Propriedades de Segurança da Informação:

A segurança da informação é garantida pela preservação de 4 aspectos essenciais:

Conceitos Básicos de SI:

-Propriedades de Segurança da Informação:

- **Confidencialidade.**

O princípio da confidencialidade é respeitado quando apenas pessoas explicitamente autorizadas podem ter acesso à informação.

Conceitos Básicos de SI:

-Propriedades de Segurança da Informação:

- **Integridade.**

O princípio da integridade é respeitado quando a informação acessada está completa, sem alterações e portanto, confiável.

Conceitos Básicos de SI:

-Propriedades de Segurança da Informação:

- **Disponibilidade.**

O princípio da disponibilidade é respeitado quando a informação está acessível, por pessoas autorizadas, sempre que necessário.

Conceitos Básicos de SI:

-Propriedades de Segurança da Informação:

- **Autenticidade.**

O princípio da autenticidade garante conhecer a identidade de um usuário ou sistema de informação. Para ter a garantia que é original. (assinatura digital, código eletrônico, criptografia).

Conceitos Básicos de SI:

-Outras Propriedades de S.I:

- **Ativo de Informação.**

A informação é elemento essencial para todos os processos de negócio da organização, portanto é qualquer coisa que tenha valor para a organização.

Conceitos Básicos de SI:

-Outras Propriedades de S.I:

- **Vulnerabilidade.**

São fraquezas presentes nos ativos de informação, que podem causar, intencionalmente ou não, a quebra de um ou mais dos 4 principais princípios da informação: CIDA.

Conceitos Básicos de SI:

-Outras Propriedades de S.I:

- **Ameaça.**

A ameaça é um agente externo ao ativo de informação, que aproveitando-se das vulnerabilidades deste ativo, poderá quebrar a confidencialidade, integridade, disponibilidade e autenticidade da informação.

Conceitos Básicos de SI:

-Outras Propriedades de S.I:

- **Probabilidade.**

A probabilidade é a chance de uma falha de segurança ocorrer levando-se em conta o grau das vulnerabilidades presentes nos ativos que sustentam o negócio e o grau de ameaças que possam explorar estas vulnerabilidades.

Conceitos Básicos de SI:

-Outras Propriedades de S.I:

- **Impacto.**

O impacto de um incidente são as potenciais consequências que este incidente possa causar ao negócio da organização.

Conceitos Básicos de SI:

-Outras Propriedades de S.I:

- **Risco.**

O risco é a relação entre a probabilidade e o impacto. É a base para a identificação dos pontos que demandam por investimentos em Segurança da Informação.

RISCO = IMPACTO * PROBABILIDADE

Conceitos Básicos de SI:

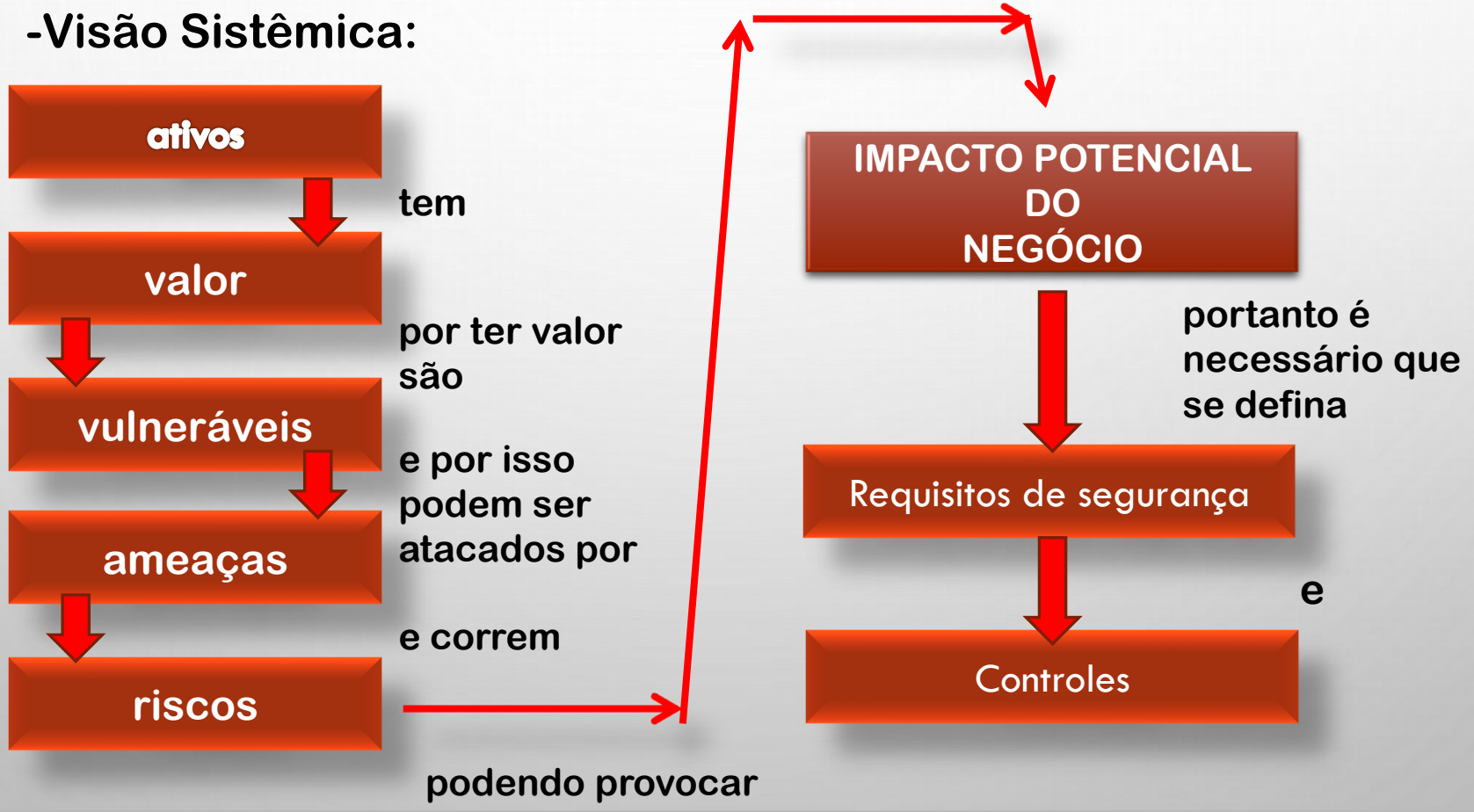
-Outras Propriedades de S.I:

- **Incidente.**

Quando uma ameaça explora vulnerabilidades de um ativo de informação, violando uma de suas características de segurança (CIDA), temos o incidente de segurança da informação.
Este incidente tem uma chance de acontecer, e se acontecer
gera um impacto ou prejuízo.

Conceitos Básicos de SI:

-Visão Sistêmica:



Análise de Risco

INTRODUÇÃO

- A INFORMAÇÃO É UM ATIVO CRÍTICO
- AMEAÇAS CIBERNÉTICAS EM CRESCIMENTO
- NECESSIDADE DE GESTÃO DE RISCOS

CONCEITOS BÁSICOS

- ATIVO, AMEAÇA, VULNERABILIDADE
- IMPACTO E PROBABILIDADE
- RISCO = COMBINAÇÃO DESSES FATORES

TRATAMENTO DE RISCOS

- MITIGAR
- TRANSFERIR
- ACEITAR
- EVITAR

Avaliação das Probabilidades

Critério	Alto	Médio	Baixo
Probabilidade da Ameaça	Ameaças comuns que ocorrem no dia-a-dia de uma empresa.	Ameaças não-comuns, mas que ocorrem com uma freqüência variável	Ameaças não-comuns, que dependem da facilidade de exploração.

Níveis de Impacto

	NIVEL DE IMPACTO		
CRITÉRIO	ALTA	MÉDIO	BAIXA
IMPACTO NO NEGÓCIO	Paralisação de processos críticos da empresa.	Alguns processos podem ser afetados. Perda de eficiência em alguns serviços do negócio.	Efeitos mínimos para o negócio.

Determinação dos Níveis de Risco

nível de risco (NR) das ameaças será estimado a partir da combinação do nível de impacto (NI) e o nível de probabilidade (NP) da ameaça

	Nível de Probabilidade (NP)	Baixa (1)	Média (2)	Alta (3)
Nível de Impacto (NI)	Alta (3)	3	6	9
	Média (2)	2	4	6
	Baixa (1)	1	2	3

Nível de Risco Alto	Nível de Risco Médio	Nível de Risco Baixo

Determinação dos Tipos de Ameaça

IDENTIFICAÇÃO DAS AMEAÇAS	
Ameaça	Tipo
Danificação do equipamento	Dano Físico
Queda do Link de Dados	Paralisação de Serviço
Acesso Indevido	Comprometimento da Informação
Indisponibilidade de Dados	Comprometimento da Informação

Identificação dos Ativos (Exemplo)

Ativo	Função
Link de Dados	Responsável pela comunicação da filial estudada, com as outras filiais, matriz e locais externos
Servidor de Arquivos	Local onde estão armazenados os arquivos dos usuários e departamentos.
Switchs (Fora do CPD)	Switchs secundários, que recebem o fluxo de informação dos switchs do backbone
Servidor Supervisório Produção	Equipamento que recebe os dados do processo de produção do negócio e envia para os computadores que realizam o monitoramento e controle

ANÁLISE DE RISCOS							
Identificação de Riscos					Estimativa de Riscos		
Nº	Ativo	Ameaça	Vulnerabilidade	Consequência	NI	NP	NR
1	Computador Supervisório E.T.A (Estação de Tratamento de Água)	Danificação de equipamento	Indisponibilidade de um equipamento backup em caso de parada do atual	Indisponibilidade do monitoramento e controle dos poços e caixa d'água (Sistema automatizado). Interrupção de processo necessário para o funcionamento do negócio.	3	2	6
2	Computador Supervisório E.T.A (Estação de Tratamento de Água)	Danificação de equipamento	Falta de uma rotina de manutenção e/ou substituição periódica	Indisponibilidade do monitoramento e controle dos poços e caixa d'agua (Sistema automatizado). Interrupção de processo necessário para o funcionamento do negócio.	3	2	6
3	Computadores Supervisório Produção	Danificação de equipamento	Falta de uma rotina de manutenção e/ou substituição periódica	Indisponibilidade de informações consideradas críticas para controle da qualidade do produto do negócio. Interrupção de processo necessário para o funcionamento do negócio.	3	2	6
4	Computadores Supervisório Produção	Danificação de equipamento	Indisponibilidade de um equipamento backup em caso de parada do atual	Indisponibilidade de informações consideradas críticas para controle da qualidade do produto do negócio. Interrupção de processo necessário para o funcionamento do negócio.	3	2	6
5	CPD (Infraestrutura Geral)	Danificação de equipamento	Falta de No-Break para estabilização da rede elétrica	Perda da eficiência do negócio. Indisponibilidade de sistemas, telefonia, rede, etc (Processos secundários do negócio)	3	1	3

Criterios Aceitação do Risco

NIVEL DE RISCO (1 - 9)	DESCRIÇÃO	ACEITABILIDADE
ALTO (6 - 9)	Os objetivos do negócio são impactados. Algum serviço necessário para o Negócio é paralisado.	Risco inaceitável. Requer ação imediata para tratamento.
MÉDIO (3 - 5)	Alguns objetivos do negócio são impactados. Alguns processos são afetados.	Risco inaceitável. Requer ação para tratamento.
BAIXO (1 - 2)	Efeitos secundários, que não causam impacto no negócio.	Risco Aceitável, nenhuma ação imediata é requerida.

Como implementar um Sistema de Segurança?

Conhecer os conceitos sobre S.I não significa saber garantir esta segurança. Alguns elaboram seus planos de segurança e acabam não atingindo os resultados desejados.
Um gerente de segurança da informação trabalha com fatos, com resultados de análise de exames da organização em questão.
A partir destes resultados, estabelece um conjunto de ações coordenadas no sentido de garantir a SI.

Conjunto de ações → conjunto de mecanismos integrados entre si um sistema de segurança da informação.

Como implementar um Sistema de Segurança?

A implantação de um Sistema de S.I.

O modelo proposto pela qualidade (família ISO) é o caminho adequado.

Este modelo é baseado no conceito da melhoria contínua (PDCA).

A implementação varia de acordo com a realidade e dimensão de cada organização, demorando entre 6 meses e um ano.

Como implementar um Sistema de Segurança?

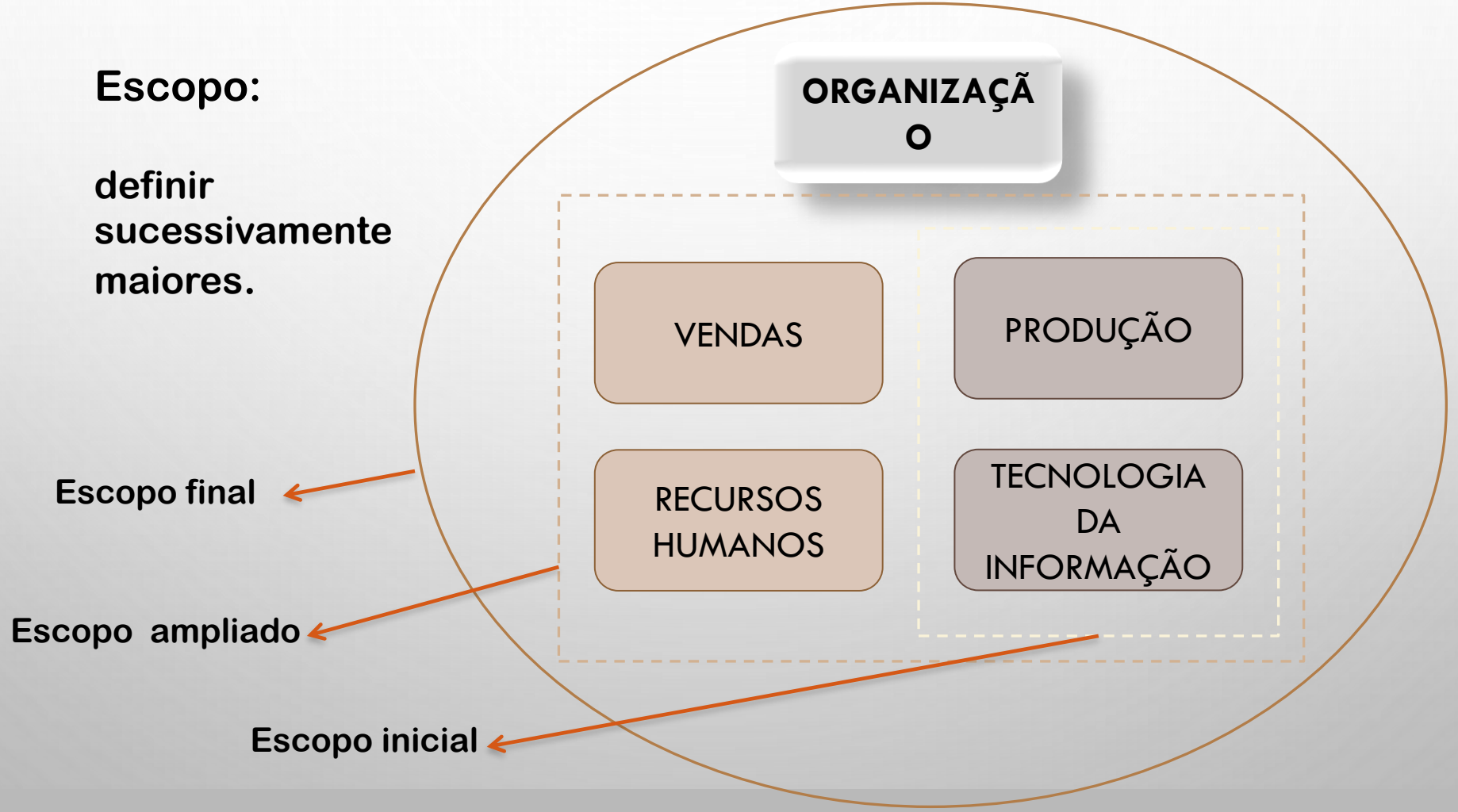
P=PLAN.

Primeira fase: o planejamento.
Nesta fase é definido o escopo e abrangência esperada para o sistema de segurança da informação, realização da análise de risco e o planejamento para o tratamento do risco.

Como implementar um Sistema de Segurança?

Escopo:

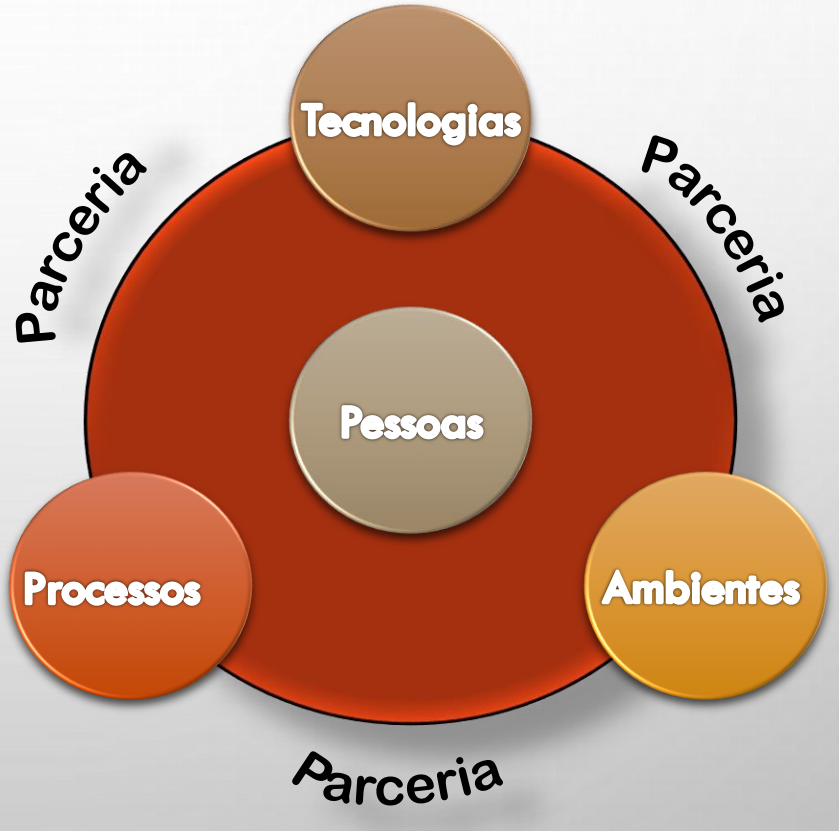
definir sucessivamente maiores.



Como implementar um Sistema de Segurança?

Análise de Risco:

Depois do escopo, decidir quais controles implementar.
A análise deve ser feita considerando as seguintes dimensões: processos, tecnologias, ambiente e pessoas; que são os ativos da Informação.
As pessoas ocupam a posição central, pois tem maior importância.



Como implementar um Sistema de Segurança?

Tratamento do risco:

com o risco identificado, o que fazer com ele?

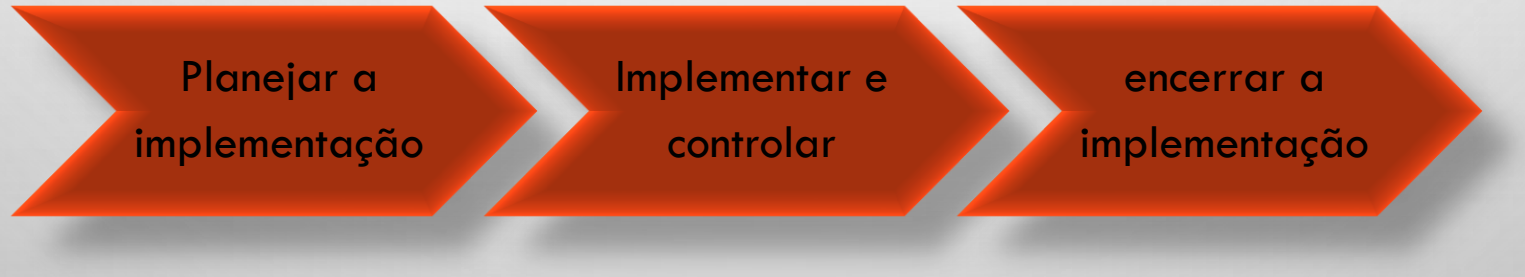
É possível:

- Evitar;
- Controlar;
- Transferir;
- Aceitar.

Como implementar um Sistema de Segurança?

D=DO=Implementar/Executar.

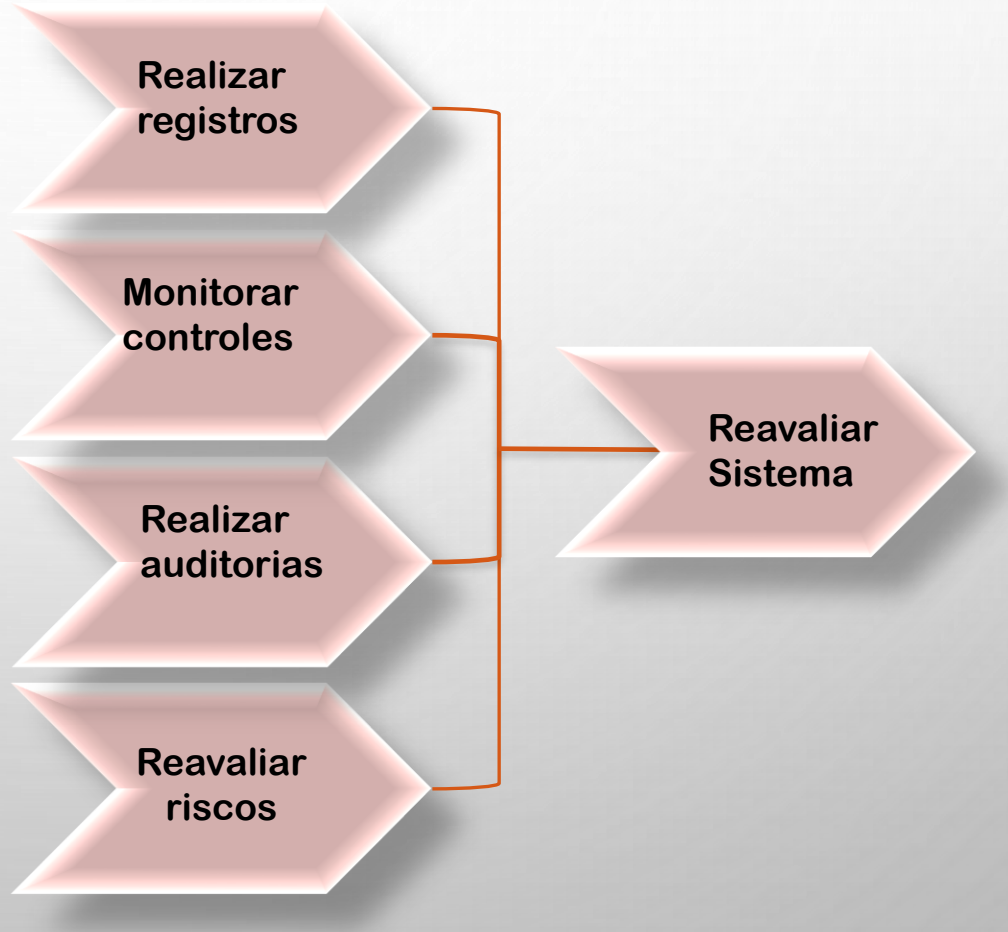
Após o planejamento o próximo passo é executar. Isto envolve o planejamento da fase de implementação, a execução e o controle da implementação e por fim, o encerramento da implementação.



Como implementar um Sistema de Segurança?

C=CHECK=Monitorar.

O monitoramento ou controle do sistema implica em avaliar sistematicamente se os controles implementados estão atendendo as expectativas originais. Os processos ao lado precisam ser executados regularmente.



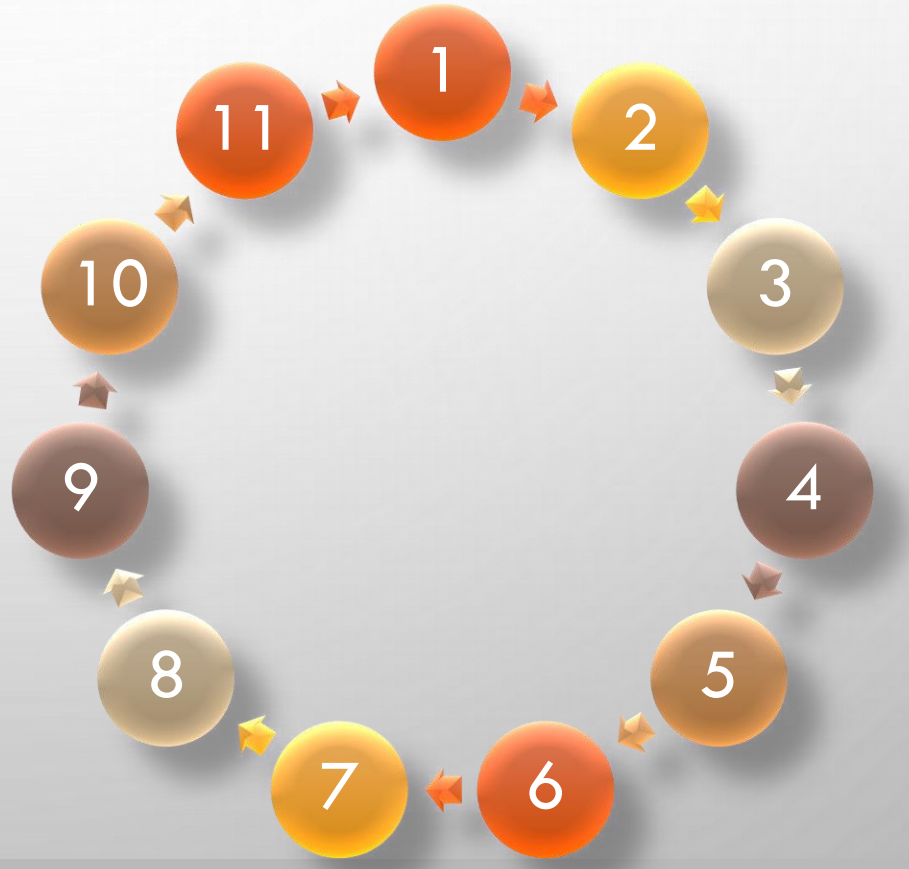
Como implementar um Sistema de Segurança?

A=ACT=Melhorar.

As atividades são corrigidas e melhoradas (aprendendo com os erros).Sistema deve ser melhorado a cada ciclo. Geralmente 1 ano e recomeça.

Controles de segurança da Informação:

1. Política (PSI);
2. Estrutura organizacional;
3. Controle de acesso;
4. Pessoas;
5. Segurança física;
6. Segurança lógica;
7. Operação de sistemas;
8. Desenvolvimento de sistemas;
9. Continuidade do negócio;
10. Incidentes de segurança;
11. Aspectos legais.



Controles de segurança da Informação:

1-Política (PSI). A Política de Segurança da Informação está estruturada em diretrizes, normas e procedimentos. Passos essenciais:

- Definições Gerais
- Objetivos e metas
- Diretrizes
- Responsabilidades
- Definições de registro de incidentes
- Frequência da revisão

- Legislação
- Regulamento interno
- Contratos

Critérios de risco

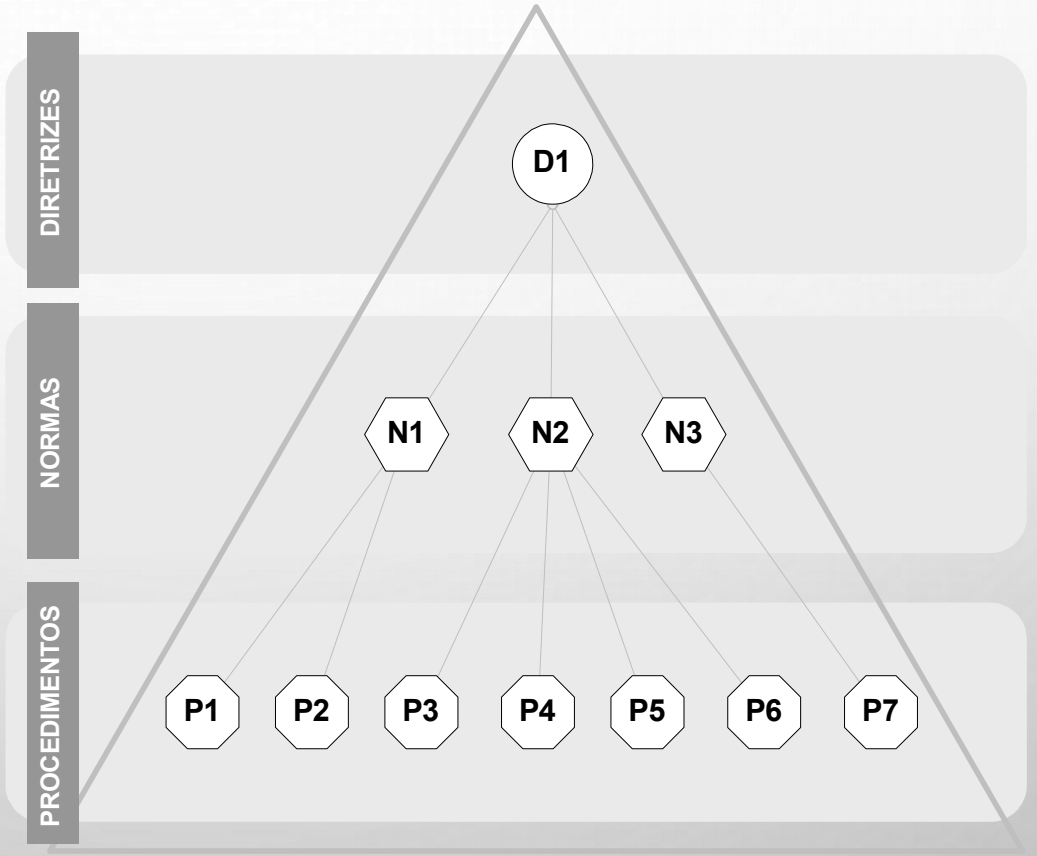
- Estabelecer o método de trabalho
- Avaliar as questões de negócio, legais e contratuais
- Definir contexto estratégico e de risco
- Construir a política
- Aprovar a política
- Divulgar a política

Política

CONTROLES DE SEGURANÇA DA INFORMAÇÃO

A política de segurança da informação (PSI) deve estar alinhada com os objetivos de negócio da organização.

Ela é estruturada em diretrizes, normas e procedimentos.



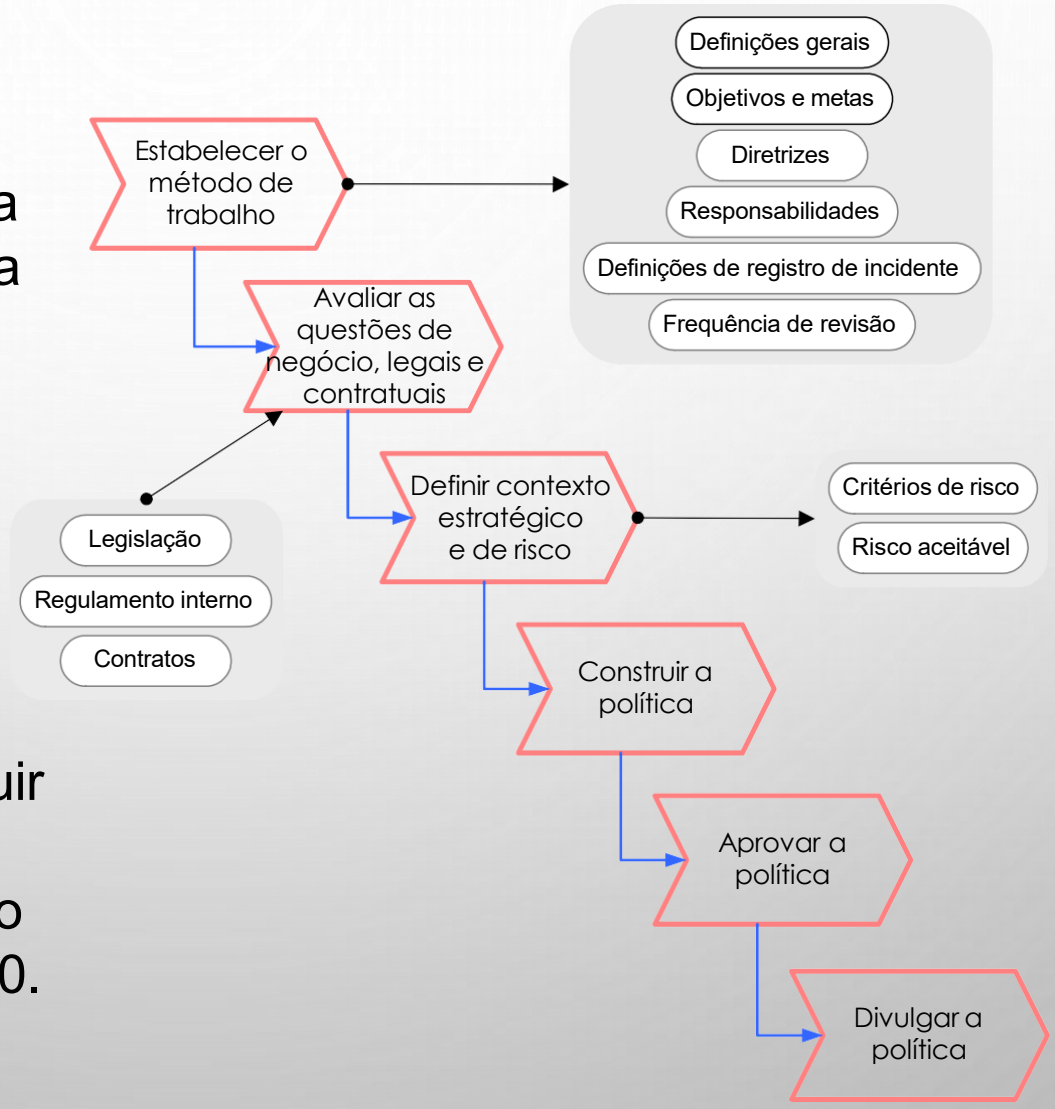
CONTROLES DE SEGURANÇA DA INFORMAÇÃO

Política

A elaboração e implantação de uma política de segurança é sem si mesmo um projeto a ser gerido.

Os passos essenciais são demonstrados na figura ao lado.

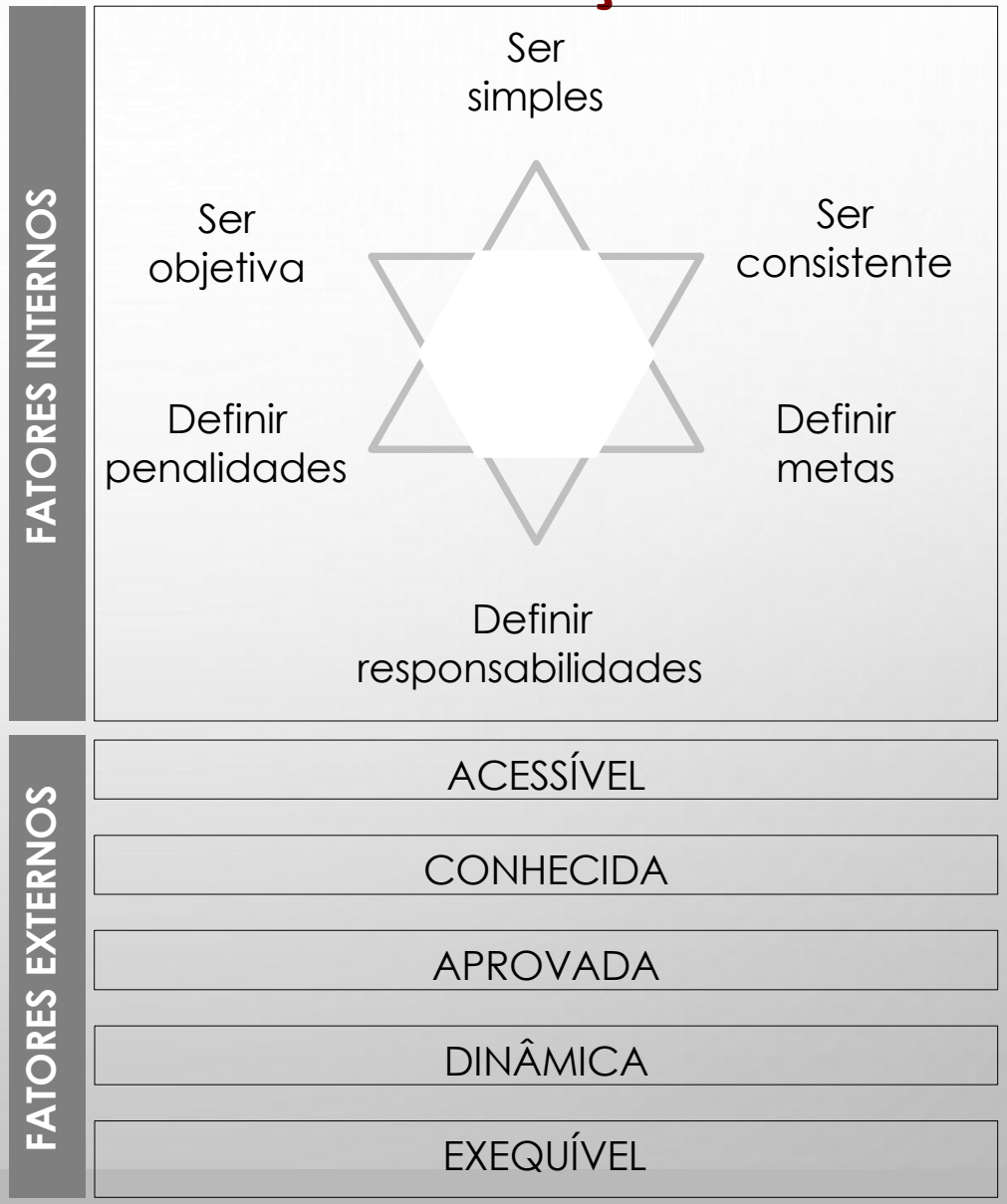
O governo federal está obrigado por decreto a possuir e respeitar uma política de segurança, conforme Decreto 3.505 de 13 de junho de 2000.



CONTROLES DE SEGURANÇA DA INFORMAÇÃO

Política

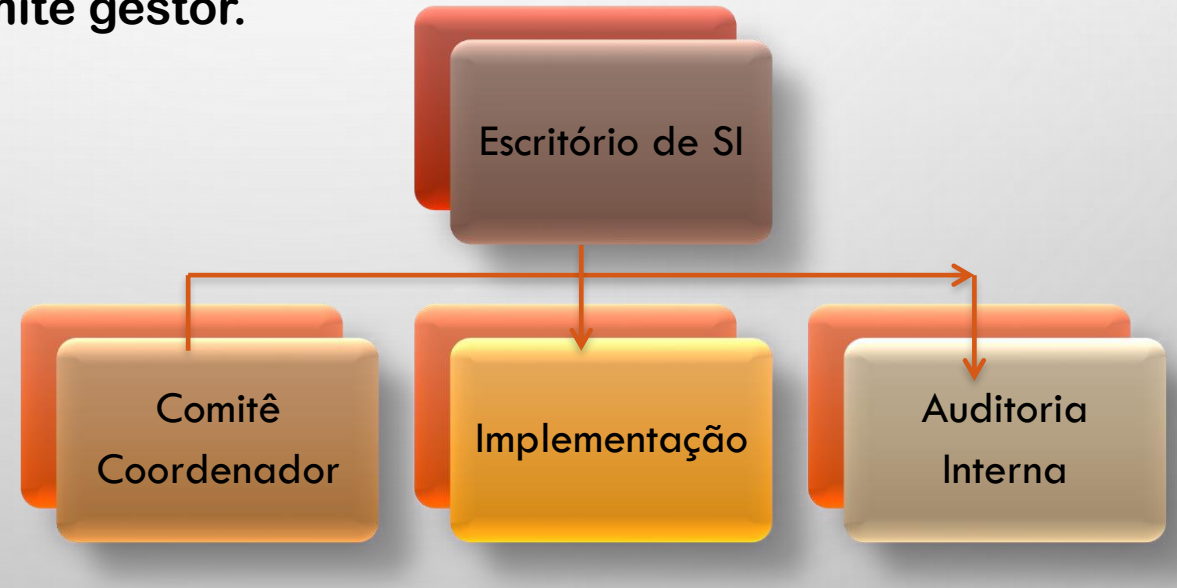
A política possui características, ou fatores, internos e externos, que precisam ser respeitados por ocasião de sua elaboração e implantação.



Controles de segurança da Informação:

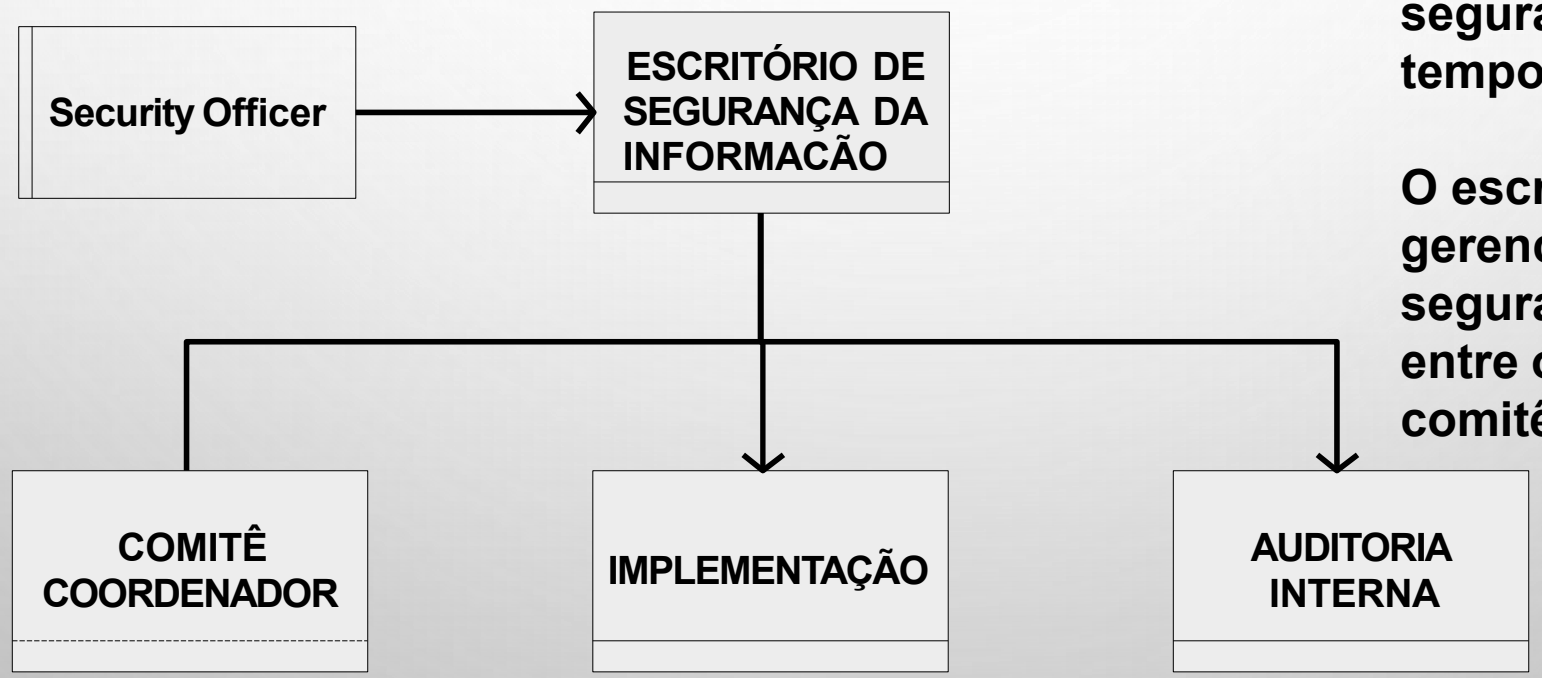
2-Estrutura Organizacional.

Deve haver uma área na organização para cuidar da SI. O escritório gerencia o sistema de segurança e faz a interlocução entre o fórum e o comitê gestor.



Escritório de segurança

ESTRUTURA ORGANIZACIONAL

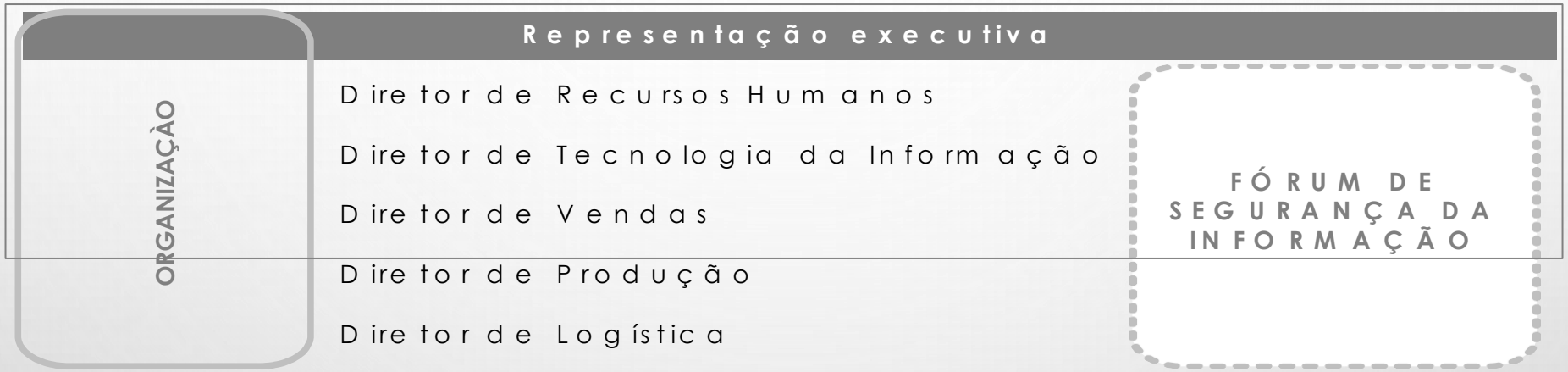


Deve haver uma área designada na organização para cuidar da segurança da informação em tempo integral.

O escritório de segurança gerencia o sistema de segurança e faz a interlocução entre o fórum de segurança e o comitê gestor de segurança.

Fórum de segurança

ESTRUTURA ORGANIZACIONAL



O fórum de segurança da informação é quem decide, em última análise, sobre a implantação ou não dos controles de segurança da informação. Este fórum, em geral, é a própria diretoria da organização, ou uma comissão por ela indicada.

Comitê gestor

ESTRUTURA ORGANIZACIONAL

O comitê gestor de segurança da informação é uma estrutura matricial formada por representantes das áreas mais relevantes da organização.

Este grupo ajuda a detectar necessidades e a implantar os controles.

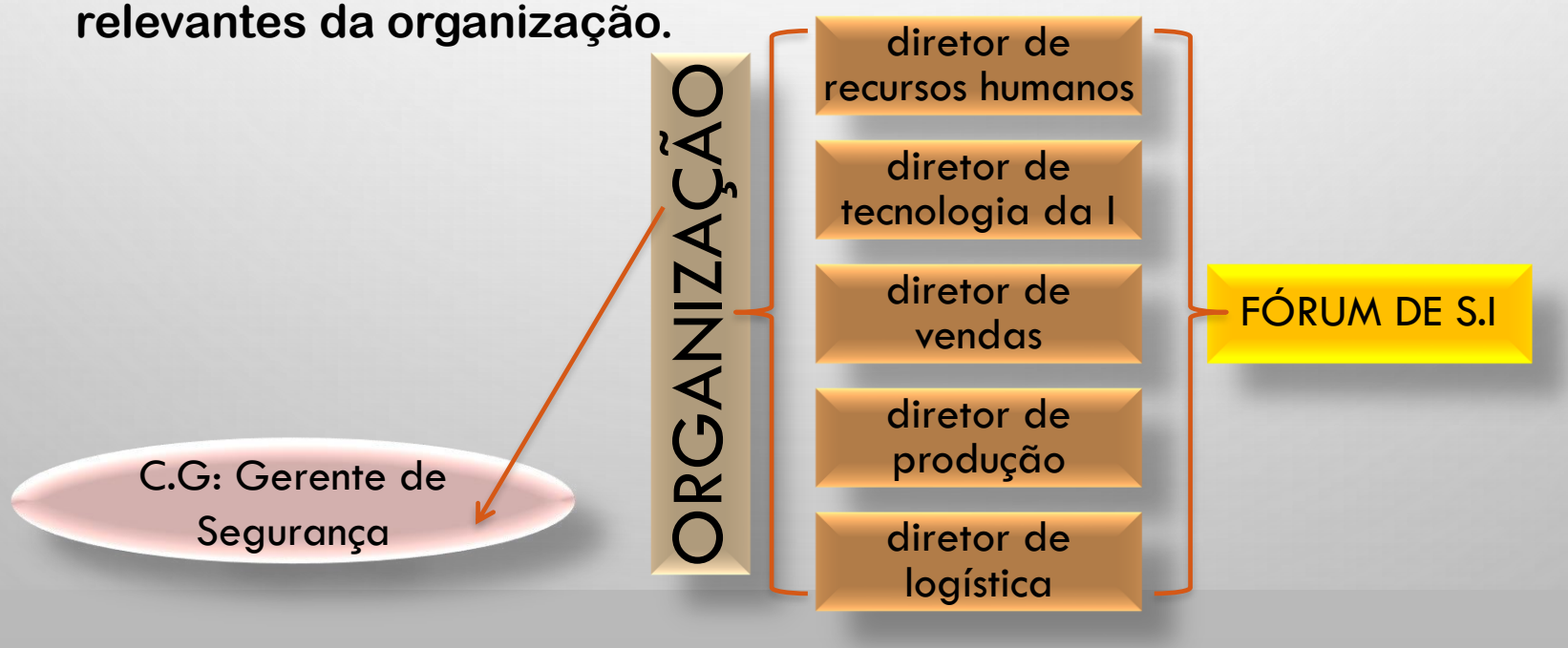
A coordenação do grupo, em geral, é do Gerente de Segurança.

Controles de segurança da Informação:

2-Estrutura Organizacional.

O fórum de SI é quem decide sobre a implantação ou não dos controles de SI. Este fórum é a própria diretoria, ou comissão por ele indicada.

O comitê gestor é formado por representantes das áreas mais relevantes da organização.



Controles de segurança da Informação:

3-Controle de acesso.

Na Idade Média já existia o conceito de controle de acesso, quando uma senha ou frase secreta era a chave para entrar em um determinado recinto. Se baseia em 2 princípios:

1-Separação de responsabilidades: implica na separação de um determinado processo de modo que cada parte possa ser realizada por uma pessoa diferente. Isto obriga uma interação entre as pessoas, diminuindo as chances de fraudes.

2-Privilégios mínimos: conhece somente o necessário para realizar suas atividades, não tendo outros conhecimentos que o levem a incidentes.

Controles de segurança da Informação:

4-Pessoas.

As pessoas são o elemento central de um S.S.I.
Os incidentes sempre envolve pessoas: vulnerabilidades + ameaças + risco. Pessoas são suscetíveis à ataques de Engenharia Social, forma de ataque mais comum. Engenharia social é o processo de mudar o comportamento das pessoas de modo que suas ações sejam previsíveis, com objetivo de obter acesso a informações e sistemas não autorizados.
Ataque de engenharia social
é realizado em 3 fases:
1-Levantamento de informações;
2-Seleção do alvo;
3-Execução do ataque.

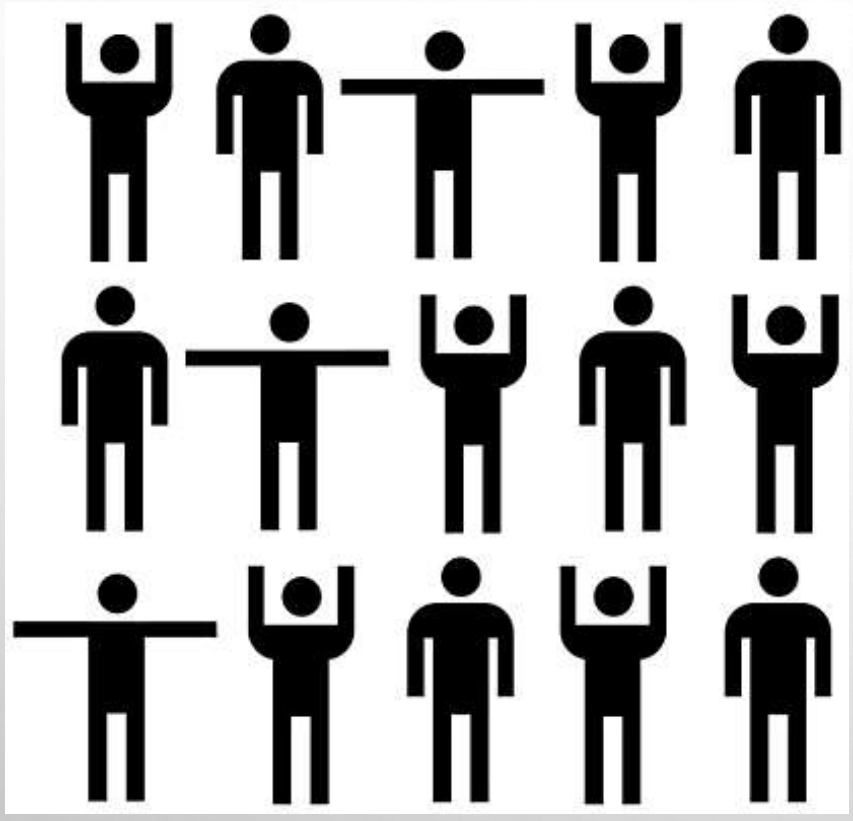
GESTÃO DE PESSOAS

As pessoas são o elemento central de um sistema de segurança da informação.

Os incidentes de segurança da informação sempre envolve pessoas, quer no lado das vulnerabilidades exploradas, quer no lado das ameaças que exploram estas vulnerabilidades.

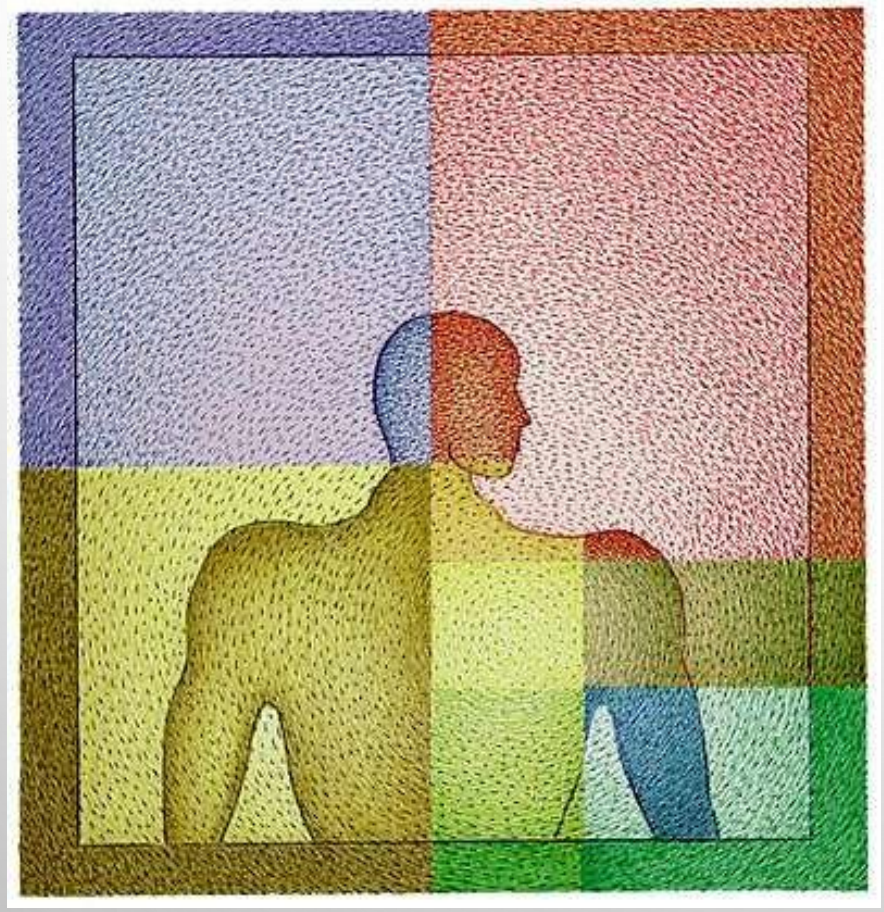
Pessoas são suscetíveis à ataques de engenharia social.

GESTÃO DE PESSOAS



A engenharia social é a forma de ataque mais comum para este tipo de ativo.

Engenharia social é o processo de mudar o comportamento das pessoas de modo que suas ações sejam previsíveis, objetivando obter acesso a informações e sistemas não autorizados.



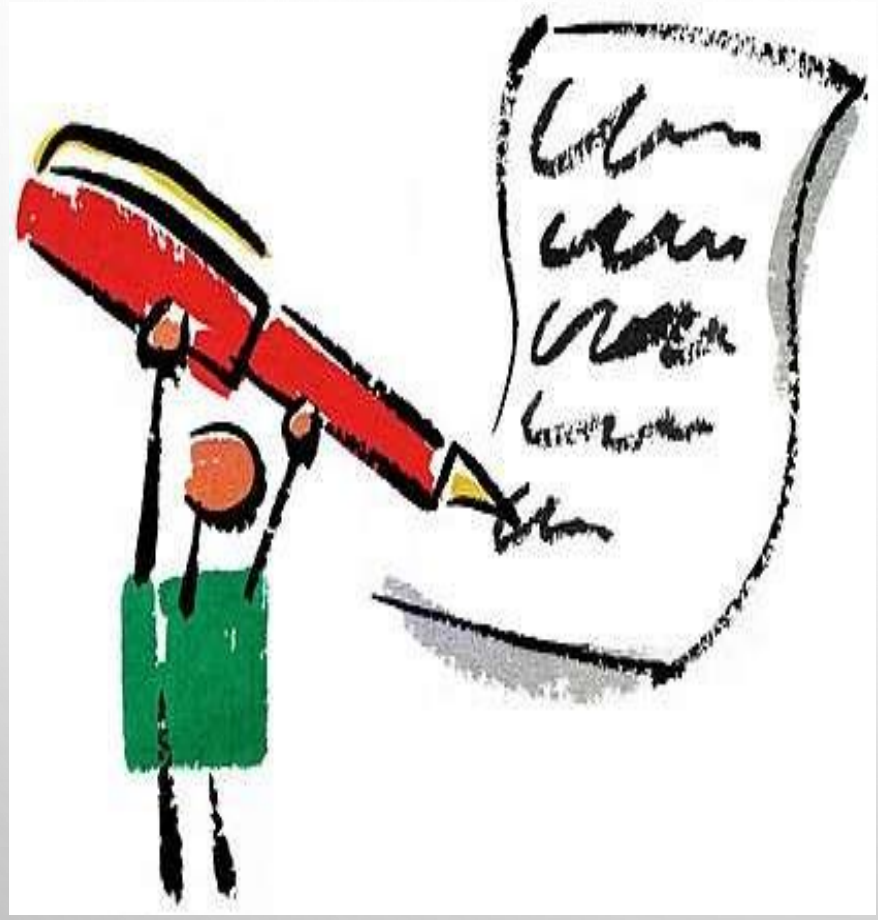
GESTÃO DE PESSOAS

Um ataque de engenharia social é realizado em três fases:

1 – Levantamento de informações;

2 – Seleção do alvo;

3 – Execução do ataque.



GESTÃO DE PESSOAS

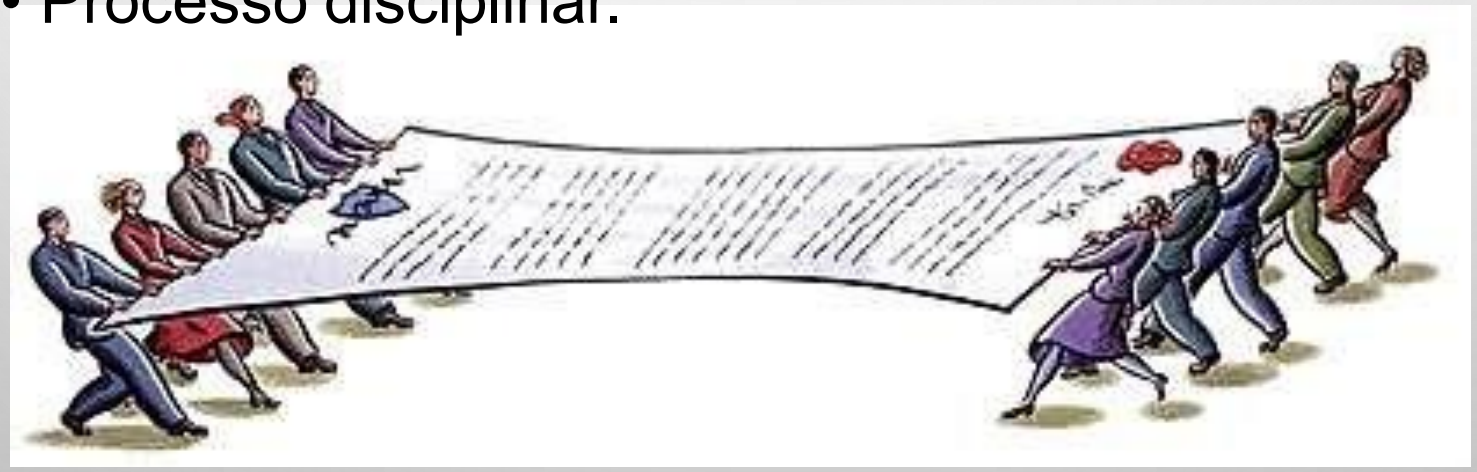
Devem ser criadas políticas para aplicação antes do contrato de pessoal.

- Papéis e responsabilidades;
- Seleção;
- Termos e condições de contratação.

GESTÃO DE PESSOAS

Políticas para aplicação durante contrato de pessoal.

- Responsabilidades da Direção;
- Conscientização e treinamento;
- Processo disciplinar.



GESTÃO DE PESSOAS

E políticas para aplicação no encerramento do contrato de pessoal.

- Encerramento de atividades;
- Devolução de ativos;
- Retirada dos direitos de acesso.

Controles de segurança da Informação:

5-Segurança Física.

As políticas de segurança física devem proteger os ativos, que sustentam os negócios da organização. A informação está distribuída fisicamente em equipamentos móveis, tais como: laptops, celulares, impressoras, telefones, estações de trabalho etc. Esta segurança deve ser aplicada para as seguintes categorias de ativos:

-Sistemas estáticos: instalações em estruturas fixadas no espaço;
-Sistemas móveis: instalados em veículos ou mecanismos móveis;
-Sistemas portáteis: podem ser operados em qualquer lugar.

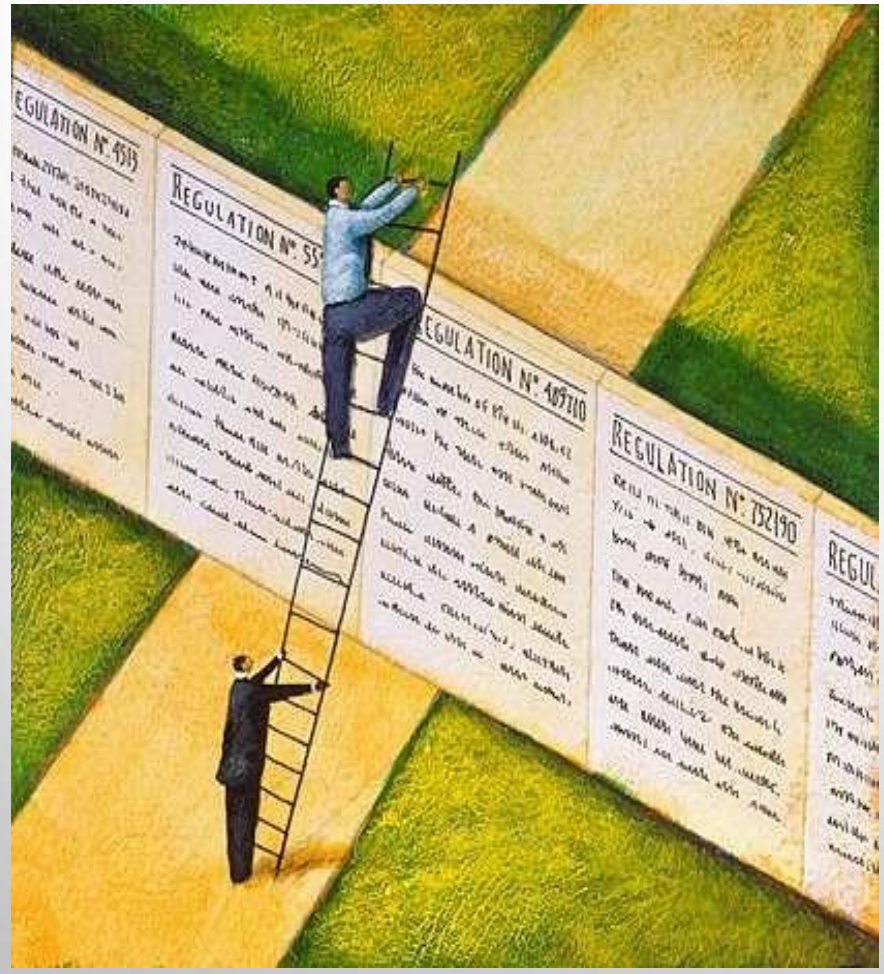
Controles de segurança da Informação:

5-Segurança Física.

Ameaças que exploram vulnerabilidades físicas:
-Naturais: enchentes, tempestades, vulcões, temperaturas extremas, alta umidade...
-Sistemas de apoio: comunicação interrompida, falta de energia...
-Humanas: explosões, invasões físicas, sabotagem, contaminação química...
-Eventos políticos: ataque terrorista, espionagem, greves...

Para controlar: Controle de entrada física; segurança em escritórios, salas e instalações; proteção de áreas críticas; instalação e proteção dos equipamentos; manutenção dos equipamentos...

SEGURANÇA FÍSICA



As políticas de segurança física devem proteger os ativos de informação que sustentam os negócios da organização.

Atualmente a informação está distribuída fisicamente em equipamentos móveis, tais como laptops, celulares, PDAs, memory keys, estações de trabalho, impressoras, telefones, FAXs, entre outros.

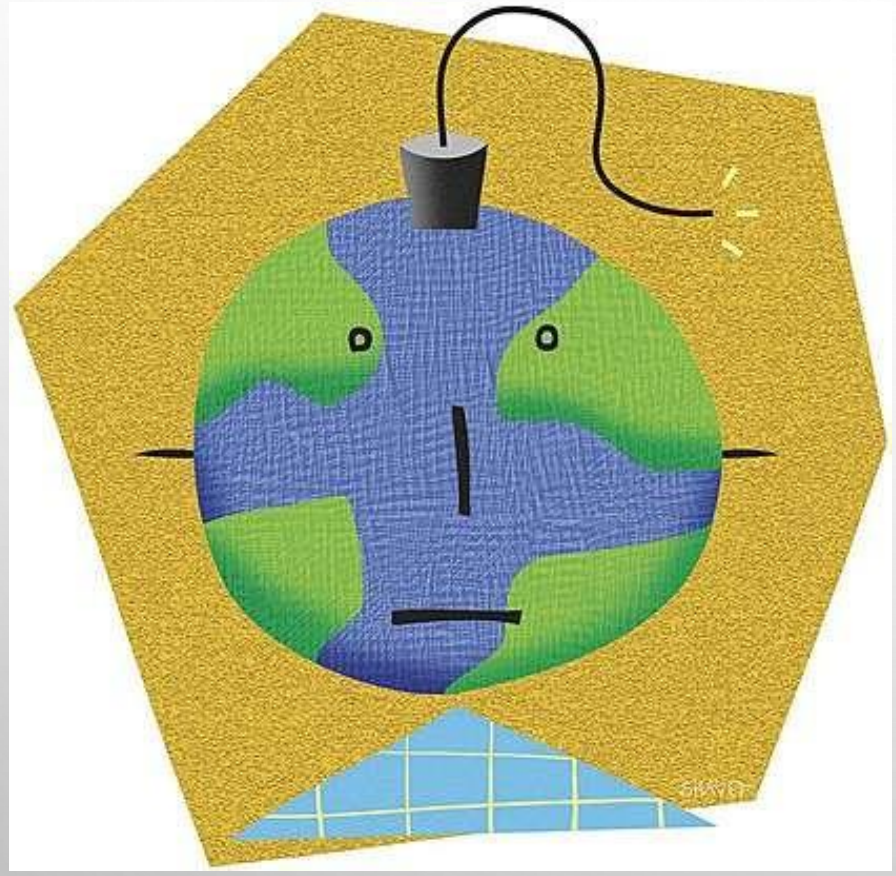
SEGURANÇA FÍSICA

A segurança física precisa garantir a segurança da informação para todos estes ativos.

Esta segurança deve ser aplicada para as seguintes categorias de ativos:

- Sistemas estáticos, que são instalações em estruturas fixadas no espaço;
- Sistemas móveis, que são aqueles instalados em veículos ou mecanismos móveis;
- Sistemas portáteis, que são aqueles que podem ser operados em qualquer lugar.

SEGURANÇA FÍSICA



Diversas ameaças que podem explorar vulnerabilidades físicas, tais como:

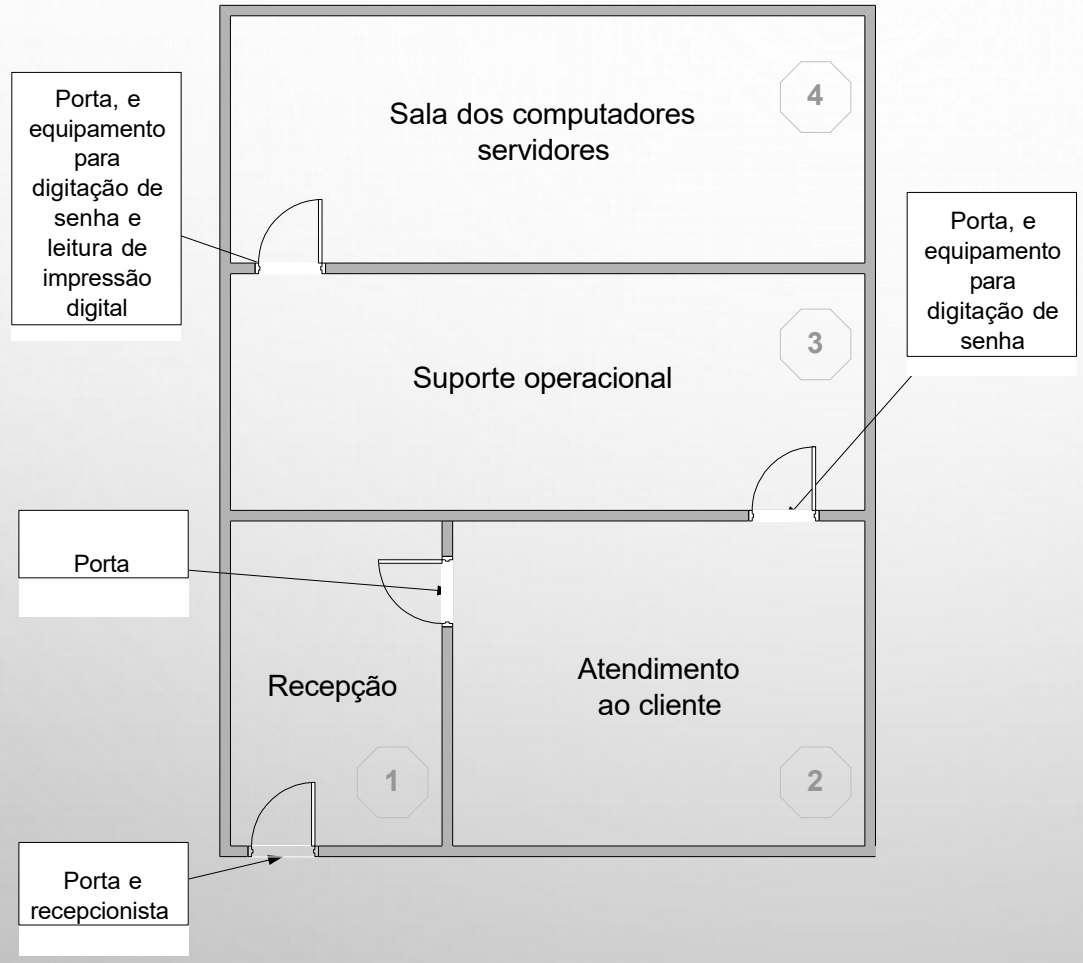
Naturais – Enchentes, tempestades, erupções vulcânicas, temperaturas extremas, alta umidade...

Sistemas de apoio – Comunicação interrompida, falta de energia, estouro em tubulações...

Humanas – Explosões, invasões físicas, sabotagens, contaminação química...

Eventos políticos – Ataque terrorista, espionagem, greves...

SEGURANÇA FÍSICA



A segurança física requer que a área seja protegida, e uma forma simples de enxergar a segurança física é definindo perímetro de segurança, ou camadas de acesso.

SEGURANÇA FÍSICA

As seguintes políticas de segurança física devem ser consideradas:

- Controle de entrada física;
- Segurança em escritórios, salas e instalações;
- Proteção contra ameaças externas e naturais;
- Proteção das áreas críticas;
- Acesso de pessoas externas;
- Instalação e proteção dos equipamentos;
- Equipamentos fora da organização;
- Estrutura de rede;
- Manutenção dos equipamentos;
- Reutilização e alienação de equipamentos;
- Remoção de propriedade.

Controles de segurança da Informação:

6-Segurança Lógica.

As informações possuem valor e usos diferenciados e precisam de graus diferenciados de proteção. A informação deve ser classificada em nível corporativo, seus benefícios são:
-CIDA é fortalecido pelos controles implementados;
-Investimento otimizado;
-Qualidade das decisões é aumentada (mais confiáveis);
-A organização controla melhor suas informações, podendo fazer uma reanálise periódica das informações.

CLASSIFICAÇÃO DA INFORMAÇÃO

As informações possuem valor e usos diferenciados, e portanto, precisam de graus diferenciados de proteção.

Cada tipo de proteção possui seu próprio custo, e classificar a informação é um esforço para evitar o desperdício de investimento ao se tentar proteger toda a informação.

CLASSIFICAÇÃO DA INFORMAÇÃO

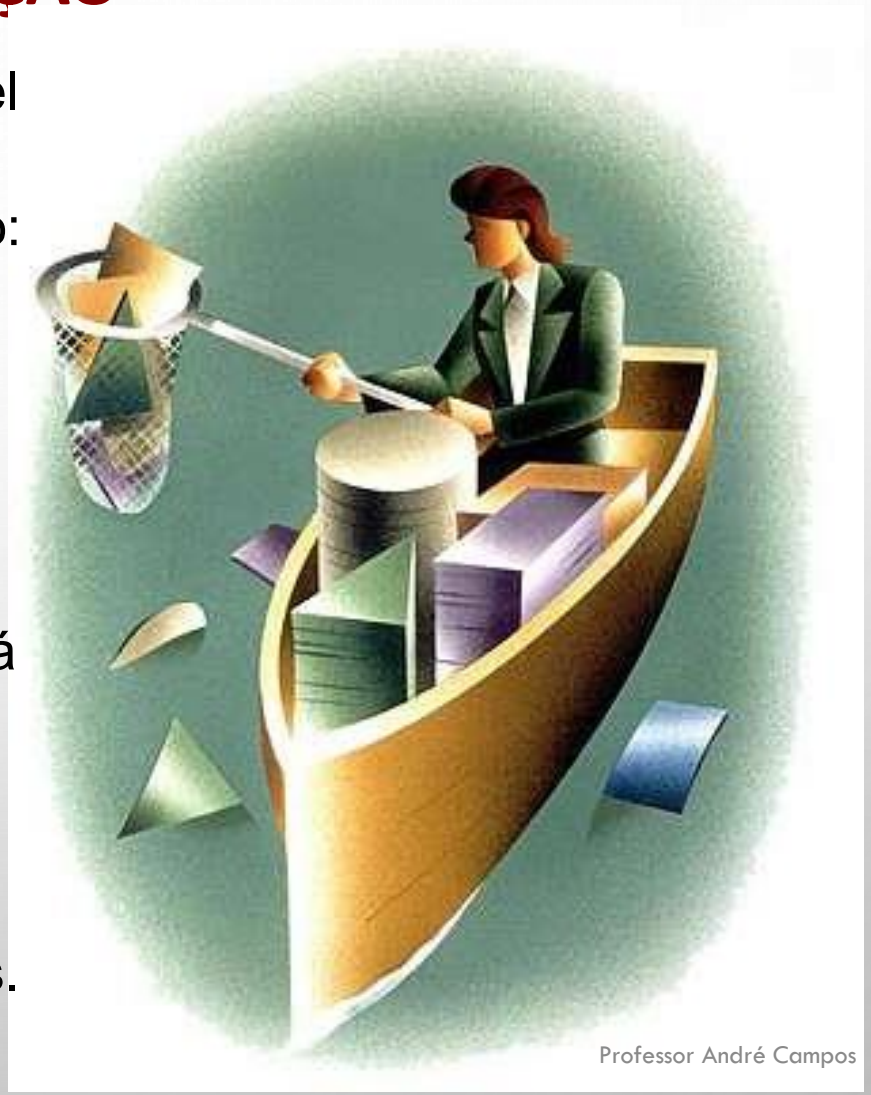
A informação deve ser classificada em nível corporativo, e não por aplicação ou departamento. Os principais benefícios são:

• CID é fortalecido pelos controles implementados em toda a organização;

• O investimento em proteção é otimizado;

• A qualidade das decisões é aumentada, já que as informações são mais confiáveis;

• A organização controla melhor suas informações e pode fazer uma re-análise periódica de seus processos e informações.



Professor André Campos

Classificação da informação

Para começar, algumas perguntas:

Existe um patrocinador para o projeto de classificação?

O que você está tentando proteger, e do quê?

Existe algum requerimento regulatório a ser considerado? (Decreto 4.554/2003)

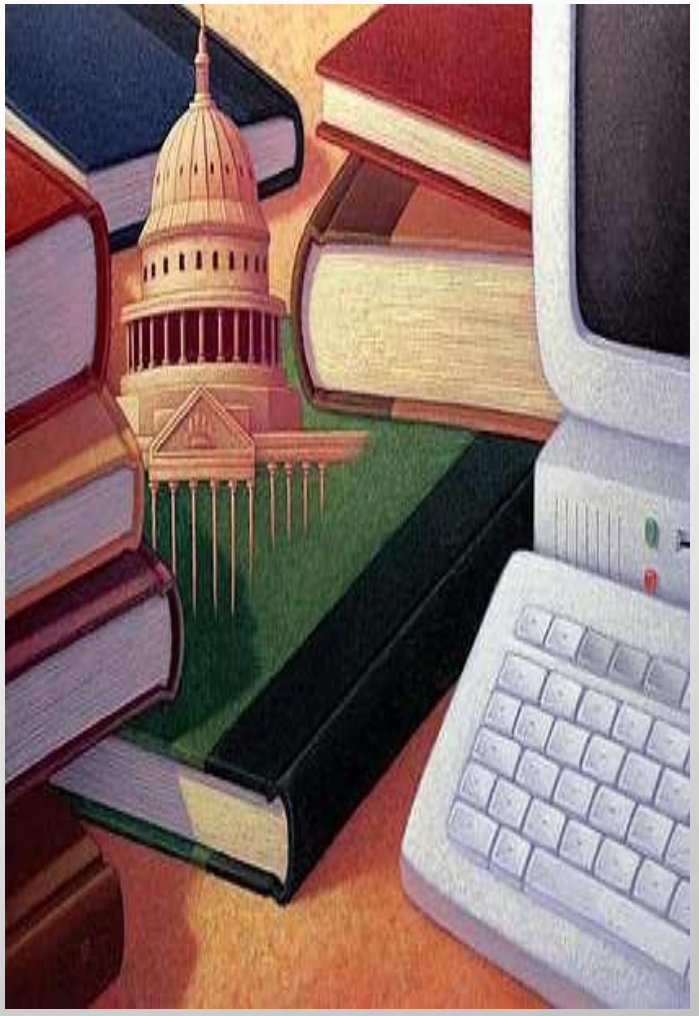
O negócio entende sua responsabilidade sobre a informação?

Existem recursos disponíveis para o projeto?

CLASSIFICAÇÃO DA INFORMAÇÃO

A política de segurança da informação deve contemplar as políticas de classificação. Alguns critérios essenciais precisam ser definidos nesta política:

- As definições para cada uma das classificações;
- Os critérios de segurança para cada classificação, tanto em termos de dados quanto em termos de software;
- As responsabilidades e obrigações de cada grupo de indivíduos responsável pela implementação da classificação e por seu uso.



CLASSIFICAÇÃO DA INFORMAÇÃO

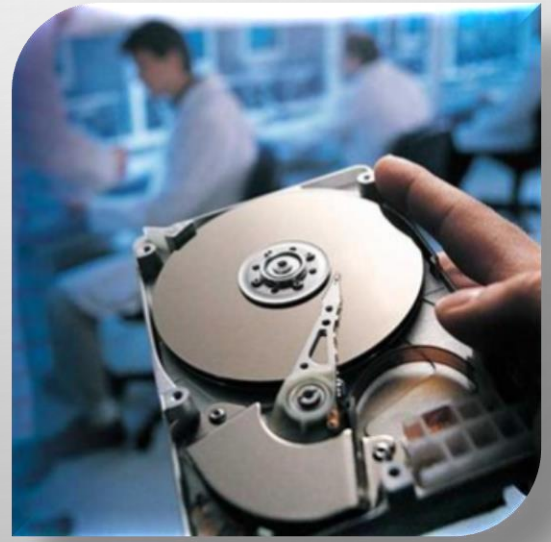
Ainda, a política precisa estabelecer as seguintes regras:

- A informação é um bem e precisa ser protegido;
- Os gerentes são proprietários da informação;
- A área de TI é custodiante da informação;
- Obrigações e responsabilidades para os proprietários da informação;
- Propor um conjunto mínimo de controles que devem ser estabelecidos.

Controles de segurança da Informação:

7-Operação de Sistemas.

As operações envolvem o controle sobre o hardware, mídias. Rede, segurança da internet, métodos de transmissão, entre outros.
O objetivo é garantir a CIDA em todas as operações. Deve existir: -registros de auditoria, monitoramento do uso dos sistemas,
proteção de informação de registro (log),
registro de log tanto do operador quanto do Administrador (criptografia), e sincronização dos relógios das máquinas;
-procedimentos para trocas de informações, (assinatura digital),
mídias em trânsito, descarte, mensagens eletrônicas...tudo deve ser gerenciado.



Controles de segurança da Informação:

8-Desenvolvimento de Sistemas.

Os procedimentos de desenvolvimento de sistemas de segurança de dados, são uma questão vital para a segurança, e para a manutenção da CIDA das informações.
A utilização de códigos abertos por comunidades é um perigo muitas vezes ignorado. O desenvolvimento de sistemas contém diversas vulnerabilidades. Se não houver uma política explícita que oriente este desenvolvimento, vulnerabilidades poderão ser introduzidas no levantamento de requisitos, na construção do projeto e na implantação do sistema.

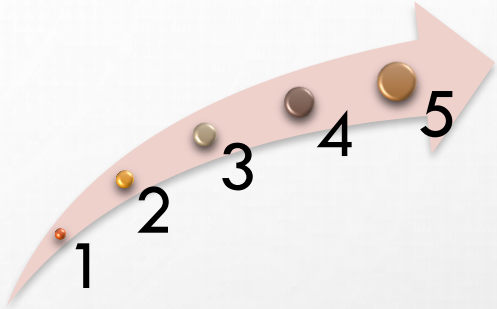
Controles de segurança da Informação:

9-Continuidade do negócio.

O plano de continuidade do negócio (PCN) é uma política para que os negócios da organização não sejam interrompidos por incidentes de S.I. Esta política deve garantir a existência de procedimentos de preparação, teste, e manutenção de ações específicas para proteger os processos críticos do negócio.

Controles de segurança da Informação:

9-Continuidade do negócio.



Um PCN é constituído de 5 fases:

1-Iniciação e gestão do projeto: onde são estabelecidos o gerente e a equipe do projeto. (que elaboram o plano).

2-Análise de impacto para o negócio: são identificados os tempos críticos dos processos da organização, e determinados os tempos máximos de tolerância de parada para estes processos *(downtime).*

3-Estratégias de recuperação: onde são identificadas e selecionadas as alternativas adequadas de recuperação para cada tipo de incidente, respeitando os tempos definidos na etapa anterior.

Controles de segurança da Informação:

9-Continuidade do negócio.

Um PCN é constituído de 5 fases:

4-Elaboração dos planos: onde são construídos os documentos, os planos de continuidade. Estes documentos são resultados da análise de impacto e estratégias de recuperação.

5-Teste, manutenção e treinamento: onde são estabelecidos os processos para testes das estratégias de recuperação, manutenção do PCN e garantia de que os envolvidos estão cientes de suas responsabilidades e devidamente treinados nas estratégias de recuperação.

Controles de segurança da Informação:

10-Incidentes de Segurança.

Apesar de todos os controles implementados, ocorrerão incidentes de S.I, que poderão indicar que alguns controles não estão sendo eficazes (bom motivo para reavaliá-los).

Política de S.I deve preocupar-se com:
1º Notificação e registro dos incidentes;
2ºTratamento e melhoria contínua.

Controles de segurança da Informação:

11-Aspectos Legais.

Todo o S.S.I com todos os seus controles, devem estar de acordo com as leis internacionais, nacionais, estaduais, municipais e regulamentações internas das organização, bem como com as normas e regulamentações do mercado. A política de S.I precisa garantir pela legislação vigente que existam mecanismos para determinar se um crime envolvendo sistemas de computadores foi cometido.

Controles de segurança da Informação:

11-Aspectos Legais.

Os principais incidentes que podem ter implicações legais:

1-Viroses e códigos maliciosos;
2-Erro humano;
3-Ataques terroristas;
4-Acesso não autorizado;
5-Desastres naturais;
6-Mau funcionamento de hardware e software;
7-Serviços indisponíveis.

Controles de segurança da Informação:

11-Aspectos Legais.

Mas como os crimes podem envolver computadores?
-Crime apoiado por computador: fraudes, pornografia infantil, etc.
-Crime específico de computador: roubo de senhas, sniffers, etc.
-Crime em que o computador é mero elemento: lista de clientes de traficantes, etc.

Controles de segurança da Informação:

11-Aspectos Legais.

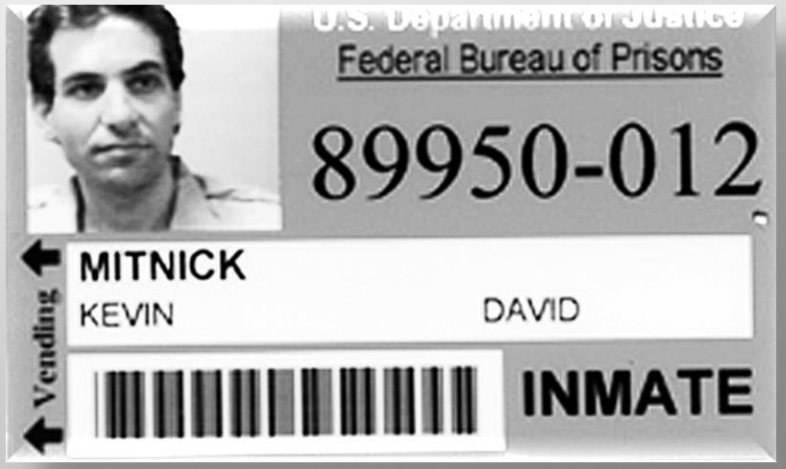
Identificação e adequação à legislação inclui: direitos de propriedade intelectual; proteção aos registros organizacionais; proteção de dados e privacidade de informações pessoais; prevenção de mau uso dos recursos do processamento da informação, e a regulamentação dos controles de criptografia.
Questões referentes à auditoria: o que garantirá a confiabilidade destas ferramentas.

Controles de segurança da Informação:

11-Aspectos Legais.

Incidente Histórico: KEVIN MITNIK, o mais famoso hacker. Mestre na arte da engenharia social, que empregava para obter acesso a muitos sistemas de computadores. Ataque direto e ataque indireto. Hoje ele presta serviço de segurança da informação.

Vulnerabilidade + ameaça + risco



Empresas Certificadas no Brasil:

1ST INFORMATION SECURITY COMPANY IN THE WORLD
1ST
ISO 27001 CERTIFIED

MODULO Solutions for GRC
Governance, Risk and Compliance

SERASA

UNISYS
imagine it. done.

SERPRO
Serviço Federal de Processamento de Dados

Matone

SAMARCO

PRODESP
Tecnologia da Informação

Telefonica

Referências Bibliográficas

https://www.**mitnicks**ecurity.com/

http://segurancadainformacao.modulo.com.br/seguranca-da-informacao

http://www.apinfo.com/artigo81.htm

http://www.profissionaisti.com.br/2013/08/politica-de-seguranca-da-informacao-conceitos-caracteristicas-e-beneficios/

http://www.oficinadanet.com.br/artigo/1307/seguranca_da_informacao_conceitos_e_mecanismos

https://cgerumblog.wordpress.com/tag/plano-de-acao/

http://www.iso27001standard.com/pt-br/tag/declaracao-de-aplicabilidade/

http://www.apcer.com.br/index.php?option=com_content&view=article&id=516:sistemas-integrados-iso-90012008-e-isoiec-270012013&catid=18:em-destaque&Itemid=85