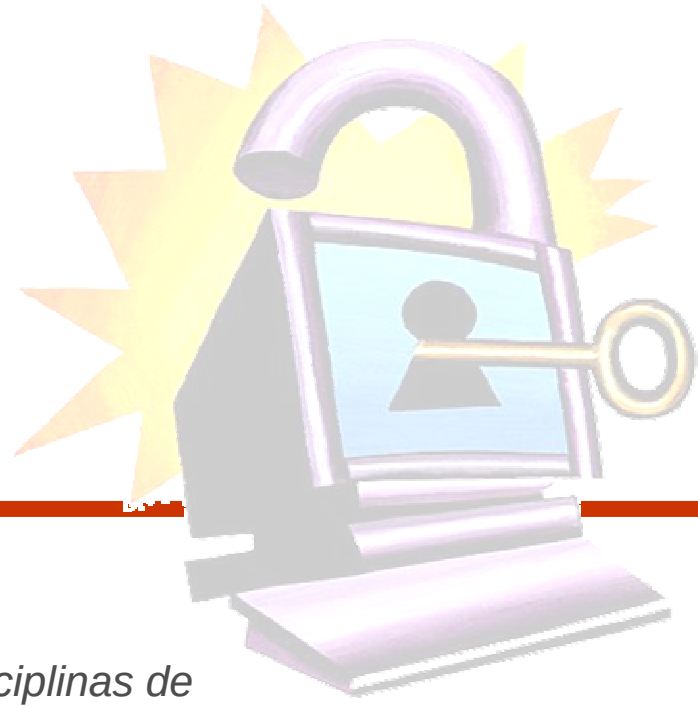
Auditoria em Tecnologia da Informação

Auditoria em Tecnologia da Informação



Este material foi produzido como apoio didático para disciplinas de graduação e pós-graduação relacionadas com segurança da informação.

O uso é permitido a todo e qualquer docente ou discente das referidas disciplinas, ou correlatas, desde que sejam respeitados os direitos autorais, ou seja, que os créditos sejam mantidos.

Este material não pode ser vendido. Seu uso é permitido sem qualquer custo.

Auditoria em Tecnologia da Informação

Crédito das imagens

Diversas figuras foram obtidas a partir do acesso público permitido pelo site www.images.com. Estas imagens foram utilizadas em seu estado original, com 72DPI, e nenhuma alteração foi aplicada sobre elas.

Algumas imagens foram obtidas da obra "Sistema de Segurança da Informação – Controlando Riscos".

Todas as imagens são utilizadas para fins exclusivamente acadêmicos e não visam a obtenção de lucro.

Auditoria em Tecnologia da Informação

Bibliografia

Sistema de segurança da informação – Controlando Riscos; *Campos, André; Editora Visual Books, 2005.*

Official (ISC)2 Guide to the CISSP exam; *Hansche, Susan / Berti, John / Hare, Chris; Editora Auerbach, 2004.*

Conceitos básicos de SI

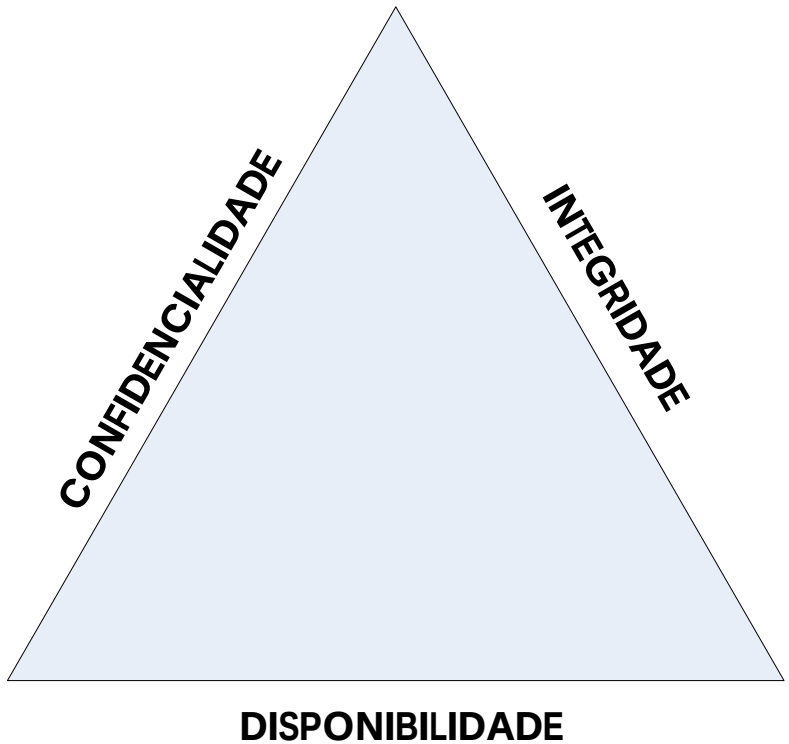
- **Ativo de informação**
- **Ameaça**
- **Vulnerabilidade**
- **Incidente**
- **Probabilidade**
- **Impacto**
- **Risco**
- **Incidente**

Ativo de informação

A informação é elemento essencial para todos os processos de negócio da organização, sendo, portanto, um bem ou ativo de grande valor.

Propriedades de segurança da informação

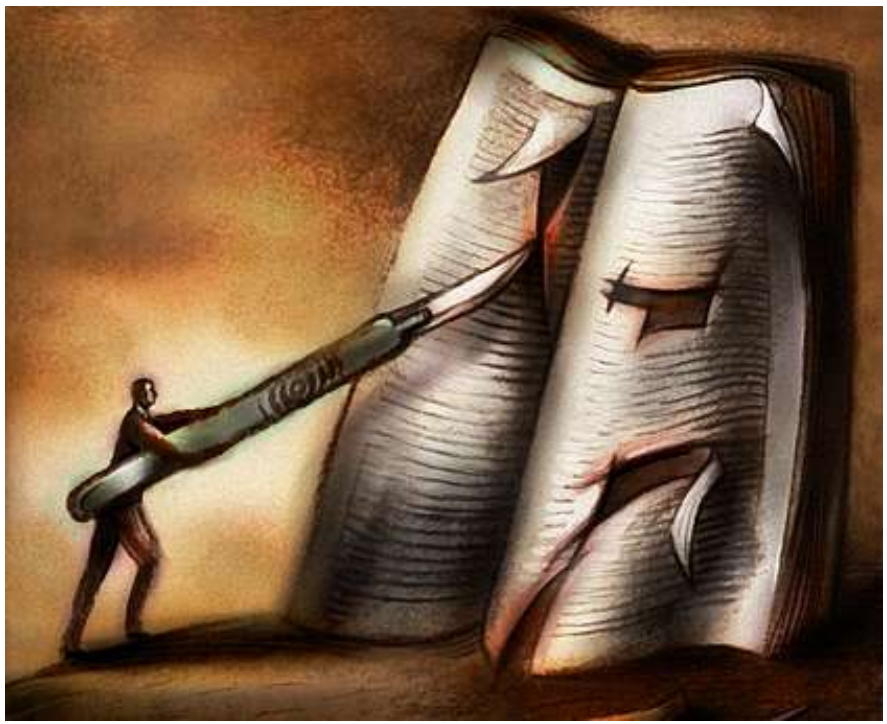
A segurança da informação é garantida pela preservação de três aspectos essenciais: confidencialidade, integridade, e disponibilidade (CID).



Confidencialidade

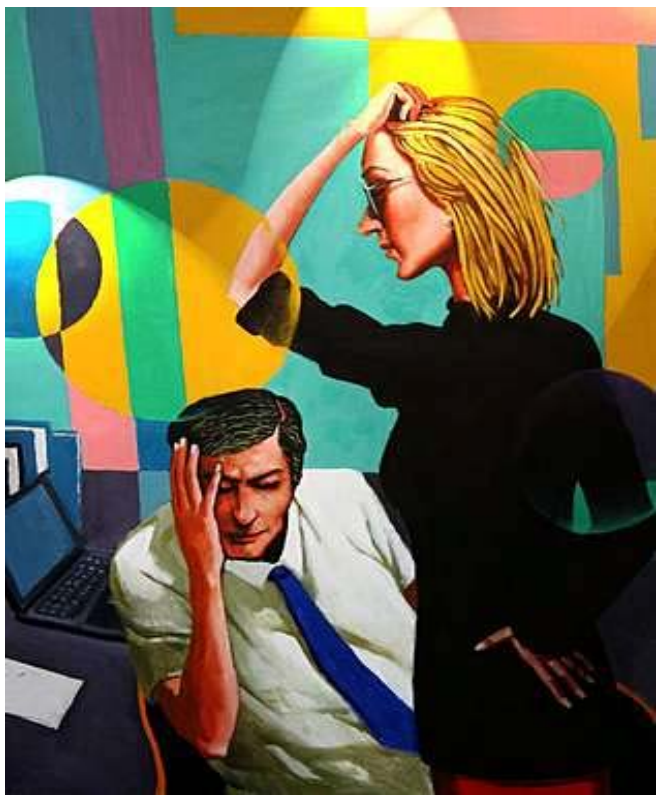
O princípio da confidencialidade é respeitado quando apenas as pessoas explicitamente autorizadas podem ter acesso à informação.

Integridade



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

Disponibilidade



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

Vulnerabilidade

São as fraquezas presentes nos ativos de informação, que podem causar, intencionalmente ou não, a quebra de um ou mais dos três princípios de segurança da informação: confidencialidade, integridade, e disponibilidade.

Ameaça

A ameaça é um agente externo ao ativo de informação, que aproveitando-se das vulnerabilidades deste ativo, poderá quebrar a confidencialidade, integridade ou disponibilidade da informação suportada ou utilizada por este ativo.

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 das ameaças que possam explorar estas vulnerabilidades.

Impacto

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

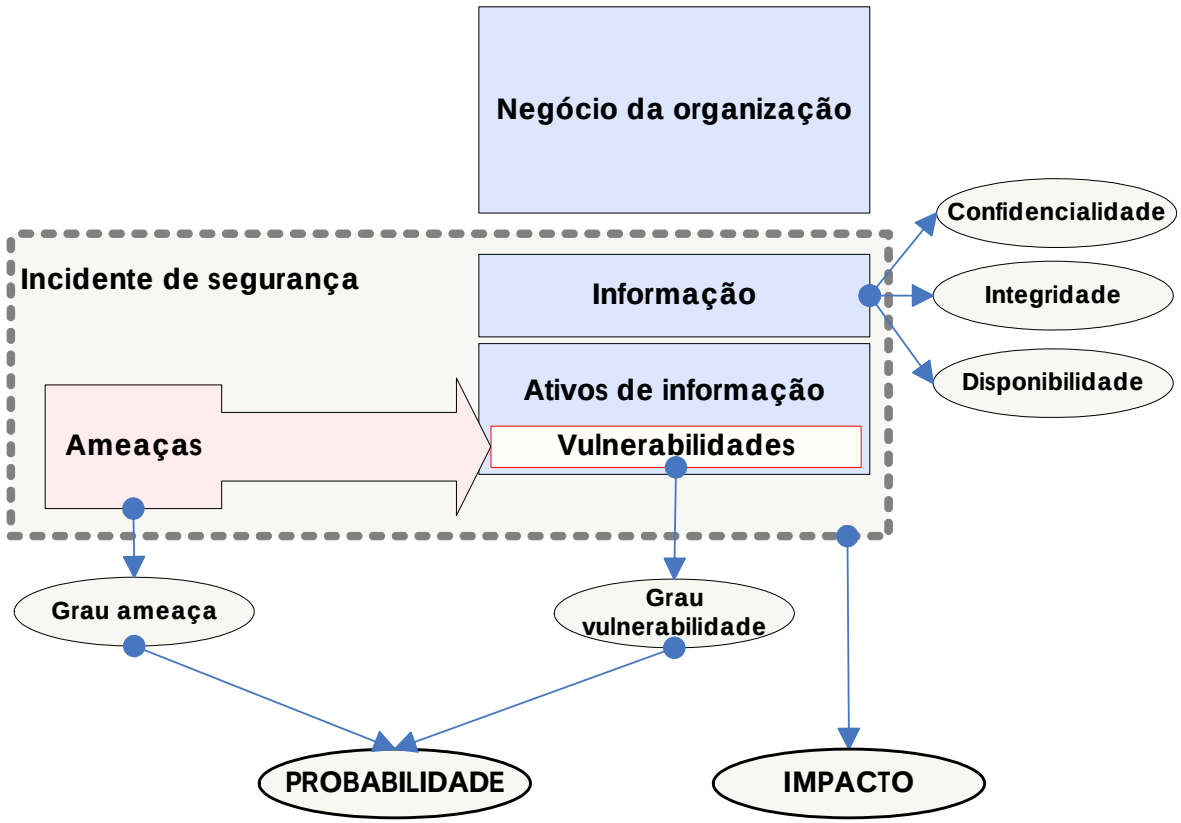
Risco

RISCO=IMPACTO*PROBABILIDADE

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.

Incidente de Segurança da Informação

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



Como implementar um sistema de segurança

Conhecer os conceitos sobre segurança da informação não significa necessariamente saber garantir esta segurança.

Muitos têm experimentado esta sensação quando elaboram seus planos de segurança e acabam não atingindo os resultados desejados.

Como implementar um sistema de segurança

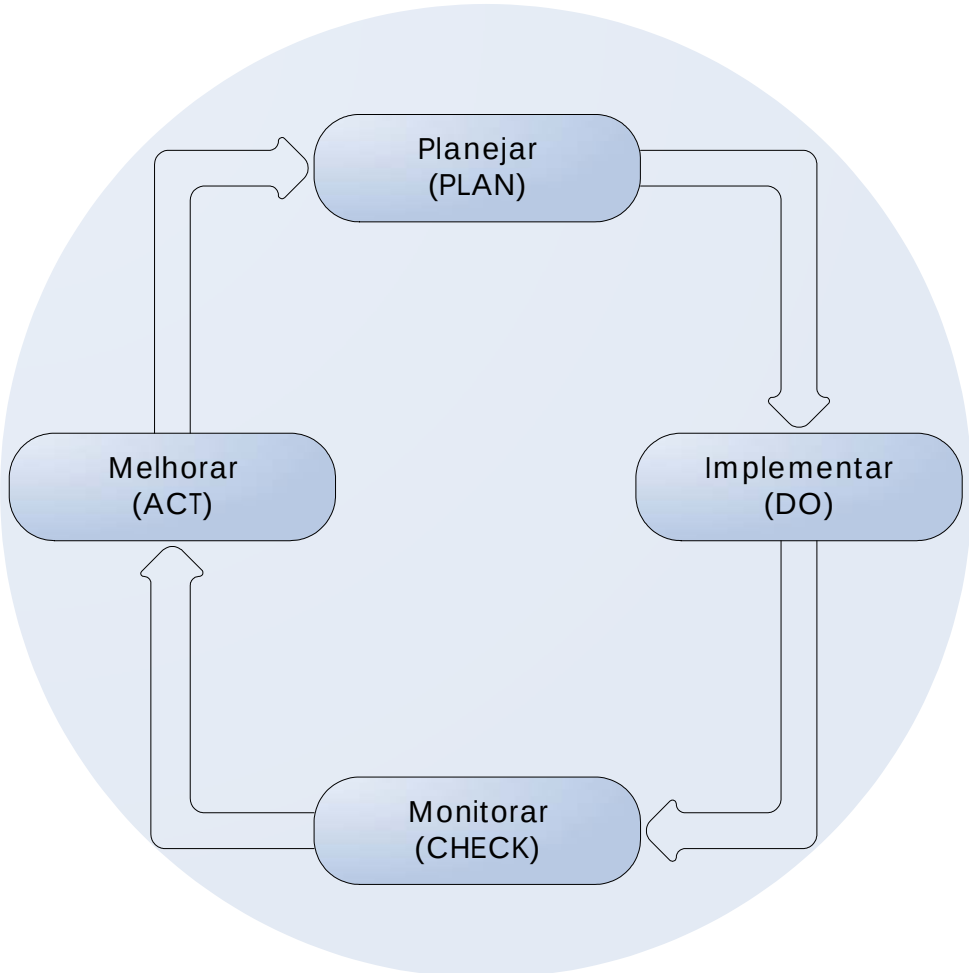
Um gerente de segurança da informação de verdade trabalha com fatos, com resultados de análise e exames da organização em questão.

A partir destes resultados ele estabelece um conjunto de ações coordenadas no sentido de garantir a segurança da informação; um conjunto de ações, um conjunto de mecanismos integrados entre si, de fato, um sistema de segurança da informação.

Como implementar um sistema de segurança

A implantação de um sistema de segurança da informação não é uma tarefa trivial.

O modelo proposto pela Qualidade (família ISO) é o caminho adequado superar este desafio. Este modelo é baseado no conceito de melhoria contínua (PDCA).

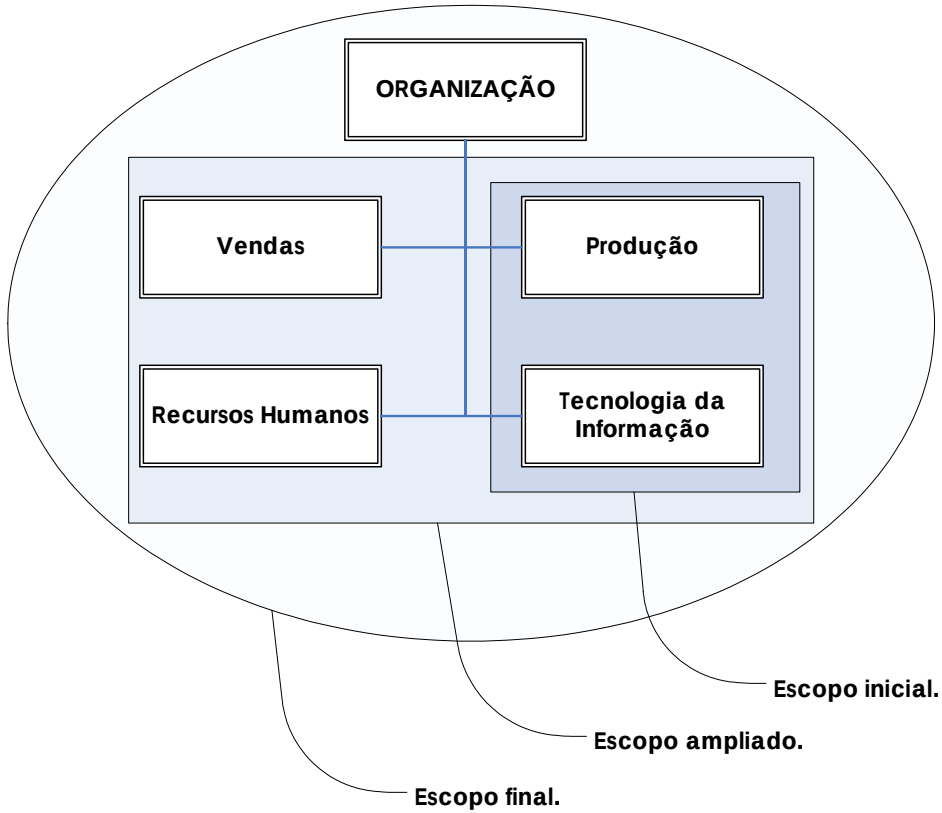


Como implementar um sistema de segurança

A primeira fase é de planejamento (PLAN). Nesta fase, é definido o escopo e abrangência esperada para o sistema de segurança da informação, e realizada a análise de risco, e feito o planejamento para o tratamento do risco.

Escopo

Nem sempre é fácil implantar o sistema em toda a organização. Por isso, definir escopos sucessivamente maiores talvez seja o caminho para se chegar ao objetivo final: segurança da informação em toda a organização.

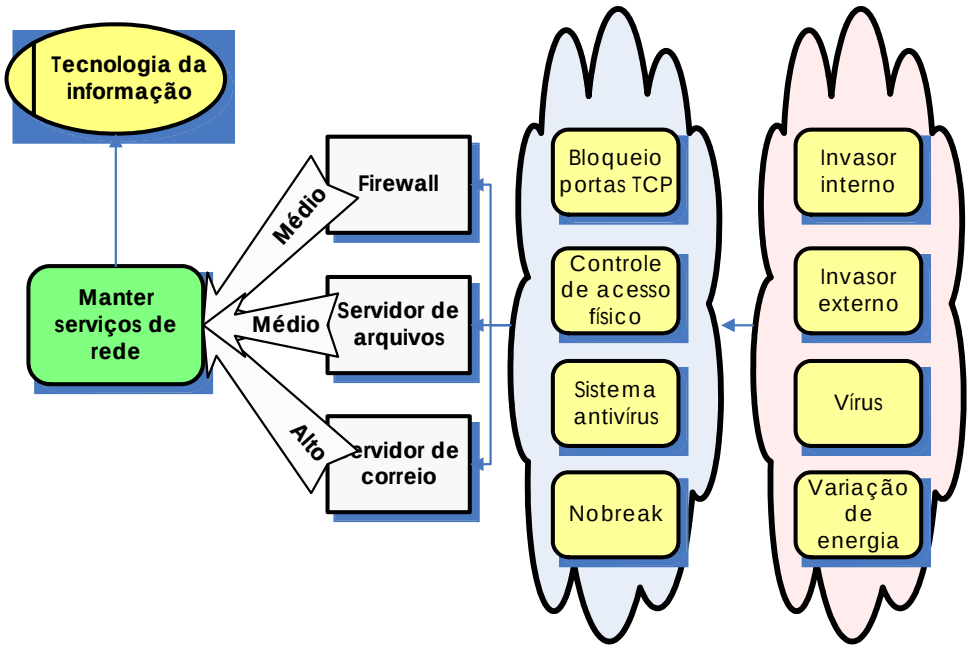


Análise de risco

Depois do escopo definido, é a hora de pensar que controles implementar.

Para otimizar esta decisão é imprescindível realizar a análise de risco. Ela apontará para as prioridades dentro do escopo.

A análise deve ser feita considerando as seguintes dimensões: processos, tecnológica, ambiental, e pessoas.



Como implementar um sistema de segurança

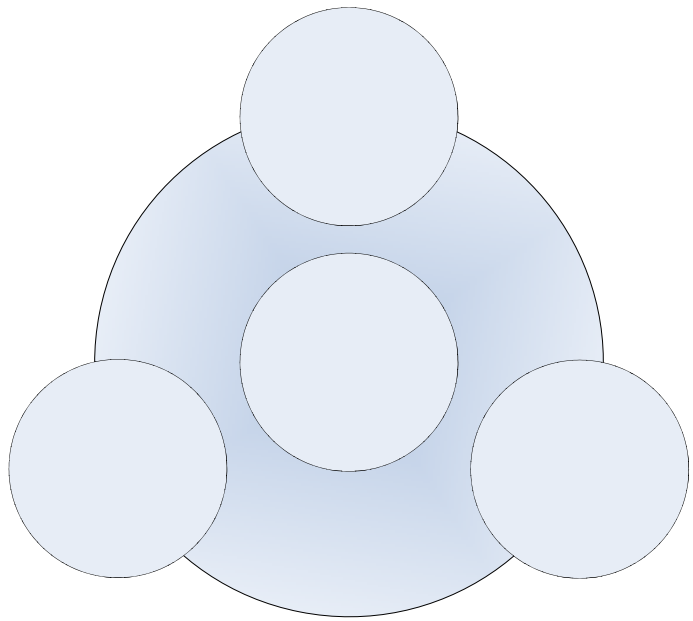
Análise de risco

120	Ativo	Impacto	Incidente	Dias/Ano	Ocorrências	Vulnerabilidade	GV	Ameaça	GE	Probabilidade	RISCO
Manter serviços de rede	Firewall	50,00%	Invasão	3	0,82%	Portas TPC abertas	80,00%	Invasor externo (hacker)	100,00%	90,00%	46,94%
				0	0,00%	Sem controle de acesso físico	60,00%	Invasor interno	10,00%	35,00%	28,33%
			Contaminação por vírus	15	4,11%	Sem sistema antivírus	10,00%	Vírus	100,00%	55,00%	36,37%
			Queda de energia	36	9,86%	Sem nobreak	10,00%	Variação de energia	50,00%	30,00%	29,95%
	Servidor de arquivos	55,00%	Invasão	0	0,00%	Portas TPC abertas	5,00%	Invasor externo (hacker)	30,00%	17,50%	24,17%
				0	0,00%	Sem controle de acesso físico	60,00%	Invasor interno	10,00%	35,00%	30,00%
			Contaminação por vírus	0	0,00%	Sem sistema antivírus	10,00%	Vírus	80,00%	45,00%	33,33%
			Queda de energia	0	0,00%	Sem nobreak	10,00%	Variação de energia	50,00%	30,00%	28,33%
	Servidor de correio	75,00%	Invasão	0	0,00%	Portas TPC abertas	50,00%	Invasor externo (hacker)	30,00%	40,00%	38,33%
				0	0,00%	Sem controle de acesso físico	60,00%	Invasor interno	10,00%	35,00%	36,67%
			Contaminação por vírus	0	0,00%	Sem sistema antivírus	10,00%	Vírus	80,00%	45,00%	40,00%

Análise de risco

Os processos, tecnologias, ambientes e pessoas são, de fato, ativos de informação; ou categorizações destes ativos.

As pessoas ocupam uma posição central entre estas categorias, pois sua importância é maior do que a das outras.



O que fazer com o risco?

Com o risco já identificado, é importante decidir o que fazer com ele. É possível:

- Evitar
- Controlar
- Transferir
- Aceitar

Isto fica claro na declaração de aplicabilidade.

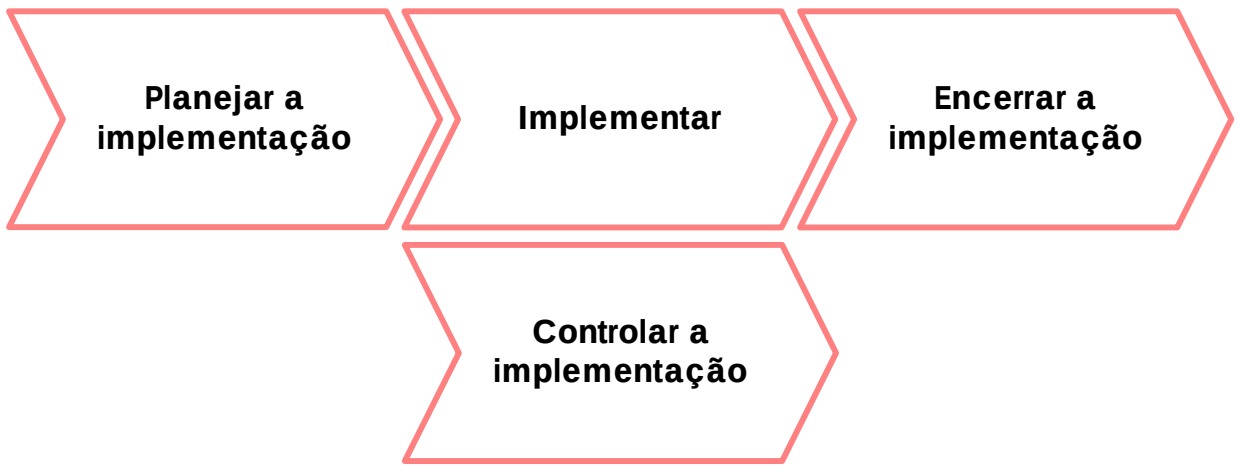
Como implementar um sistema de segurança

Declaração de aplicabilidade

Controle	Item da ISO	Objetivo	Justificativa	Prioridade da análise de risco
Fórum de segurança da informação	4.1.1	Aprovar as ações em segurança		MÁXIMA
Comitê coordenador de segurança da informação	4.1.2	Contribuir com a implantação das ações		MÁXIMA
Definição de responsabilidades sobre segurança da informação	4.1.3	Garantir o comprometimento com a segurança		MÉDIA
Autorização para aquisição de processadores de informação	4.1.4	Garantir o controle dos ativos de segurança		MÉDIA
Consultoria especializada em segurança da informação	4.1.5	**Não será implementado.**	A organização investiu em recursos internos.	MÍNIMA
Cooperação entre organizações	4.1.6	Gestão de conhecimento sobre segurança		IGNORADO
Revisão de segurança da informação independente	4.1.7	Garantir a qualidade do sistema de segurança da informação da organização		IGNORADO
Identificação de risco do acesso de terceirizados	4.2.1	Controlar as informações que são acessadas		ALTA
Requisitos de segurança em contratos de terceirização	4.2.2	Garantir a segurança da informação na relação com terceiros através da assinatura de contratos		ALTA
Requisitos de segurança em contratos de *outsourcing*	4.3.1	Garantir a segurança da informação na relação com terceiros através da assinatura de contratos		ALTA

Implementando o sistema

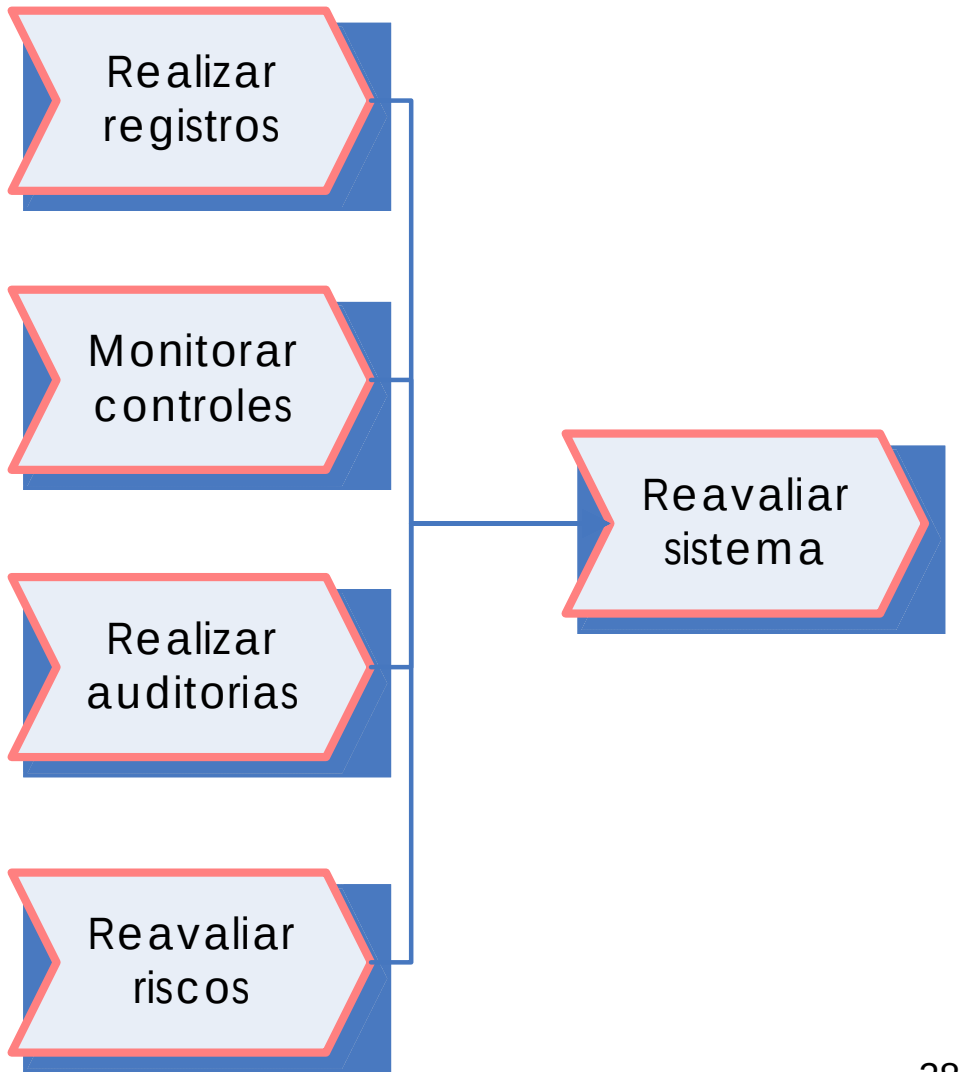
Após a etapa de planejamento, o próximo passo é executar o planejado. Isto envolve o planejamento da fase de implementação, a execução e o controle da implementação, e por fim, o encerramento da implementação.



Monitorando o sistema de segurança

O monitoramento ou controle do sistema implica em avaliar sistematicamente se os controles implementados estão atendendo as expectativas originais.

Para tanto, os processos ao lado precisam ser executados com regularidade.



Controles de segurança da informação

A implementação de um sistema de segurança da informação se dá pela instalação de controles específicos nas mais diversas áreas da organização, sempre pensando nas dimensões de processos, tecnologias, ambientes e pessoas.

Controles de segurança da informação

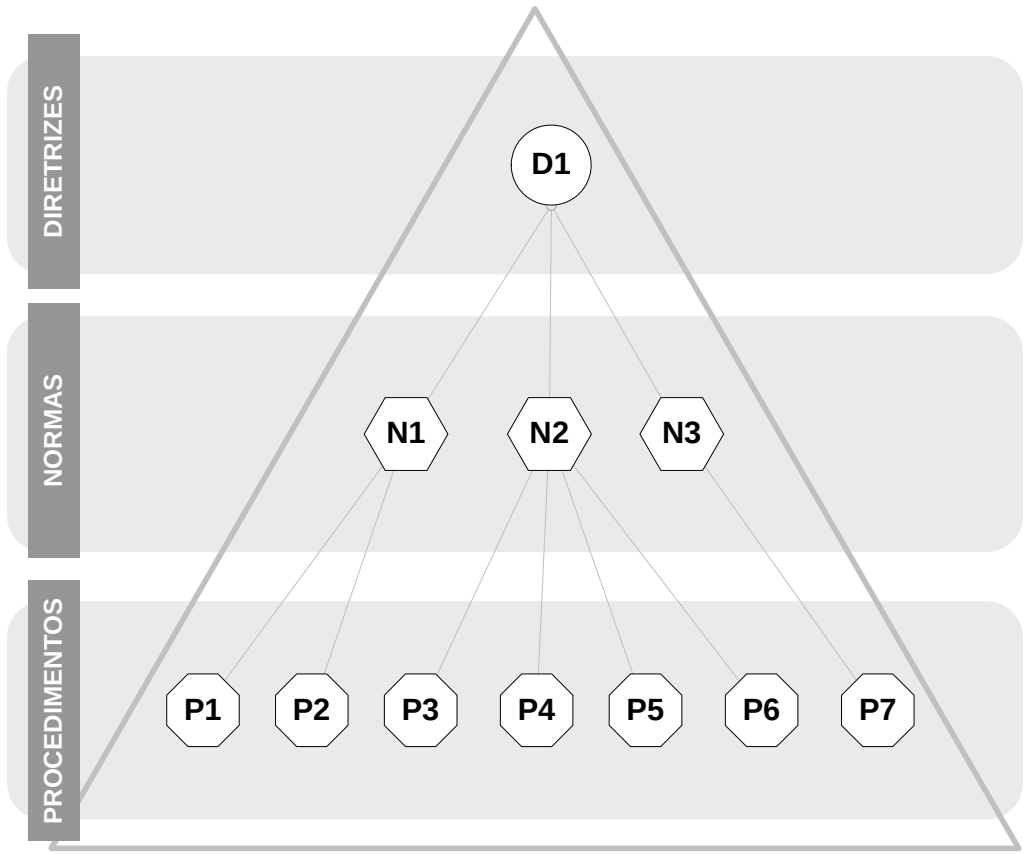
- Política (PSI)
- Estrutura organizacional
- Controle de acesso
- Pessoas
- Segurança física
- Segurança lógica
- Operação de sistemas
- Desenvolvimento de sistemas
- Continuidade do negócio
- Incidentes de segurança
- Aspectos legais

Política de segurança da informação

Política

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.

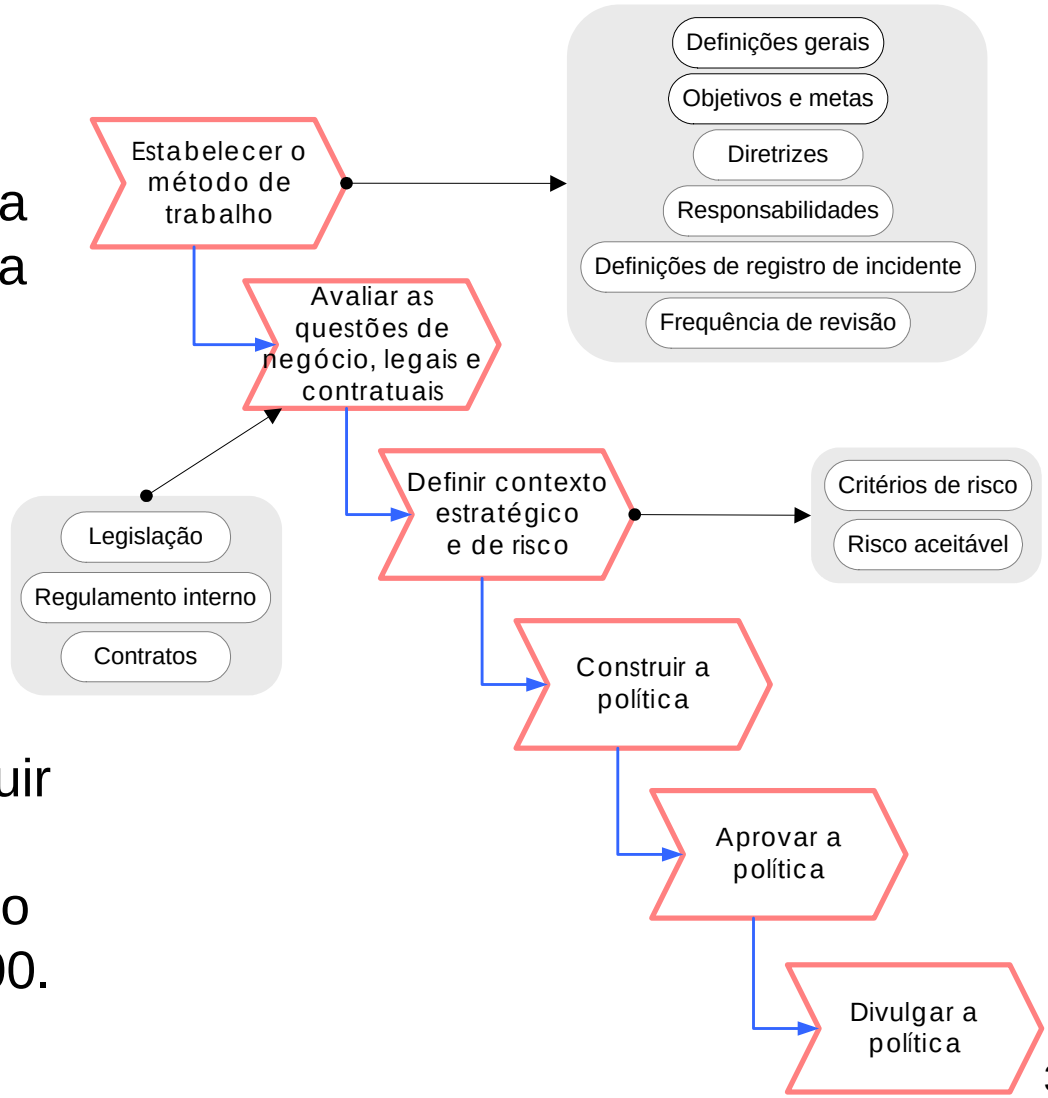


Política

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.

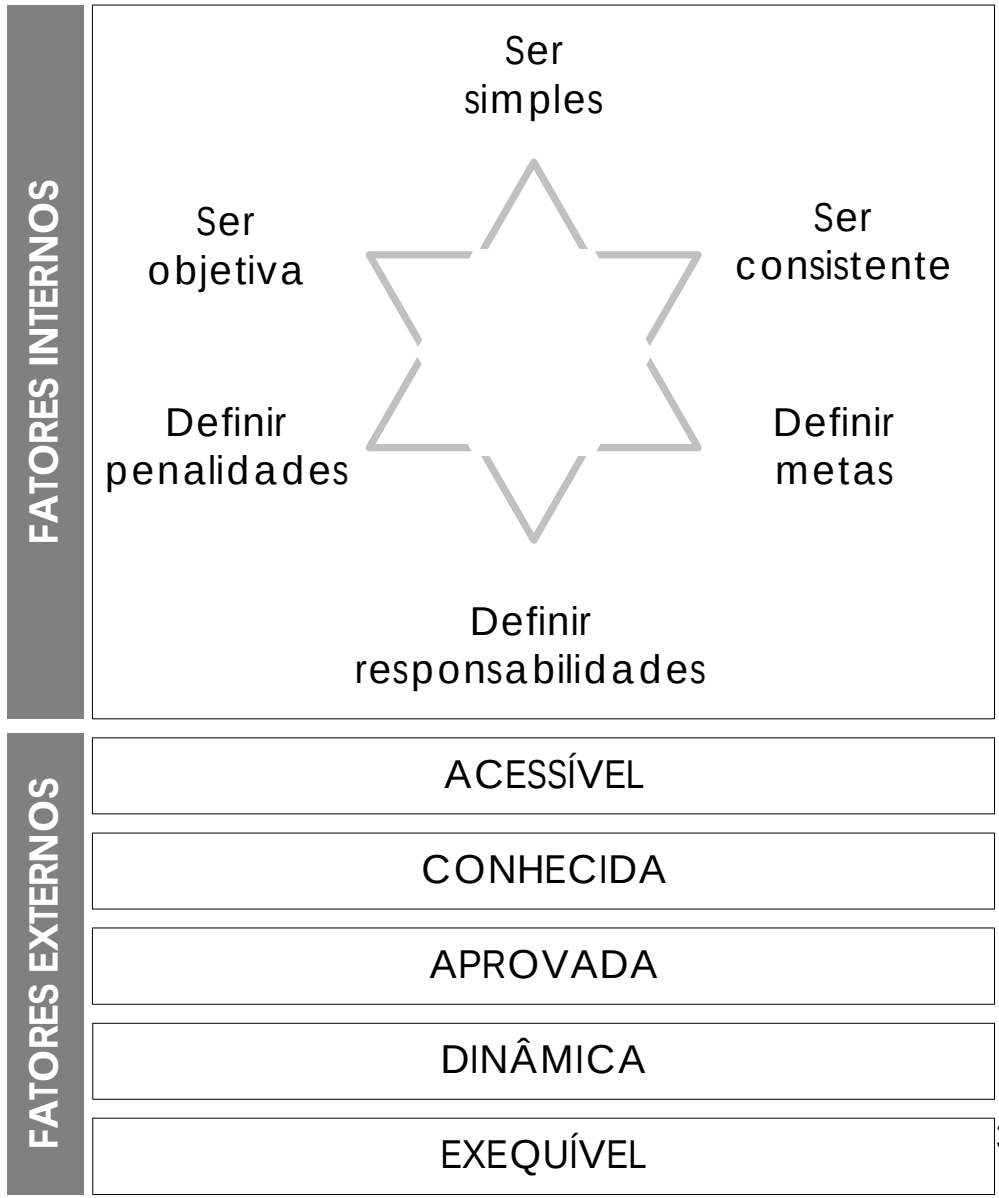
O governo federal está obrigado por decreto a possuir e respeitar uma política de segurança, conforme Decreto 3.505 de 13 de junho de 2000.



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.



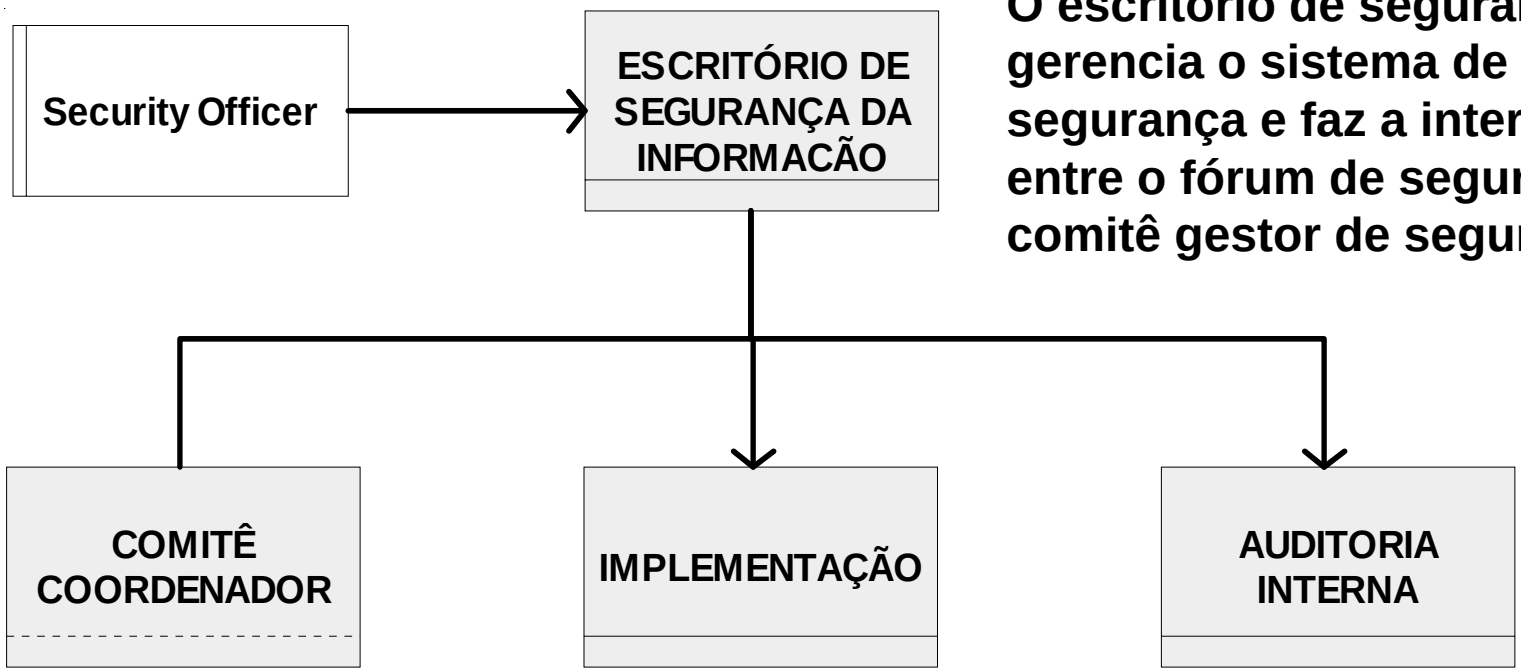
Estrutura organizacional

Estrutura organizacional

Escritório de segurança

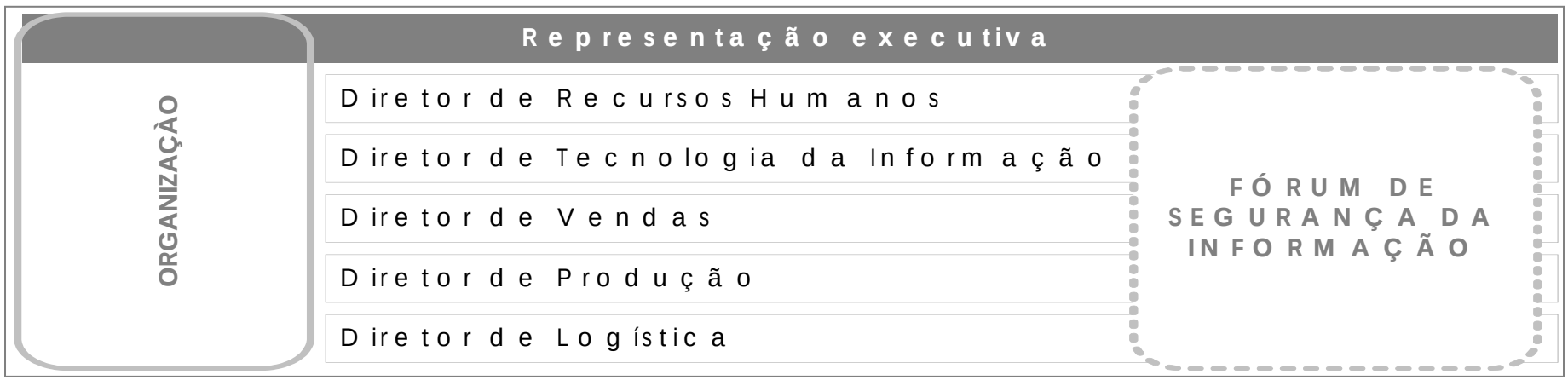
Deve haver uma área designada na organização para cuidar da segurança da informação em tempo integral.

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



Estrutura organizacional

Fórum de segurança



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

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.

Classificação da informação

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.

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)

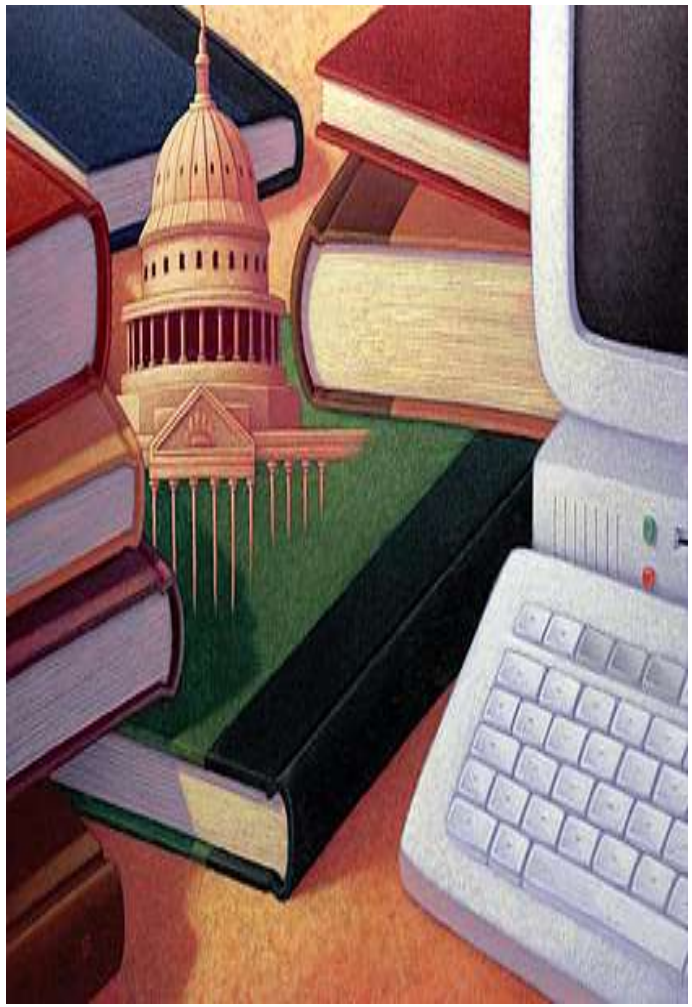
O negócio entende sua responsabilidade sobre a informação?

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.

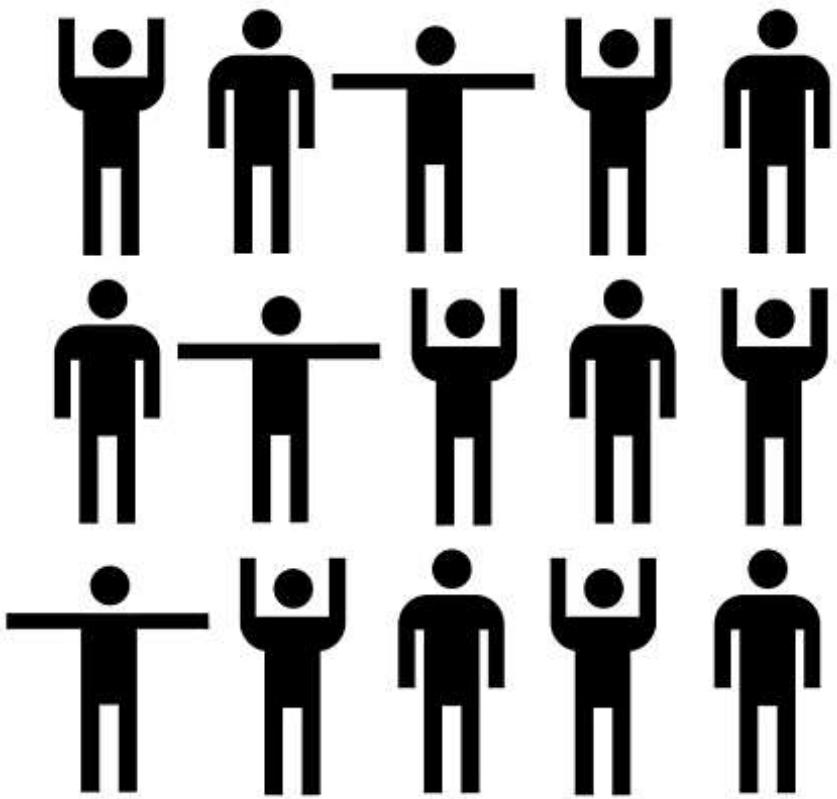
Gestão das pessoas

Gestão de pessoas

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

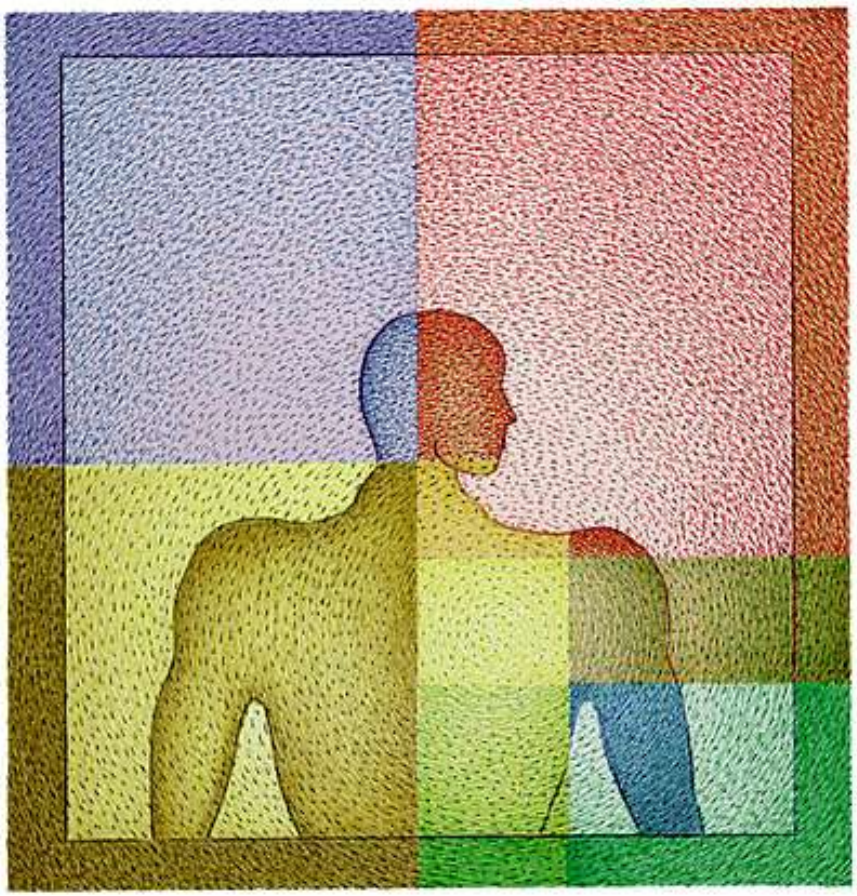
Os incidentes de segurança da informação sempre envolve pessoas, quer no lado das vulnerabilidades exploradas, quer no lado das ameaças que exploram estas vulnerabilidades.

Pessoas são suscetíveis à ataques de engenharia social.



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.



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

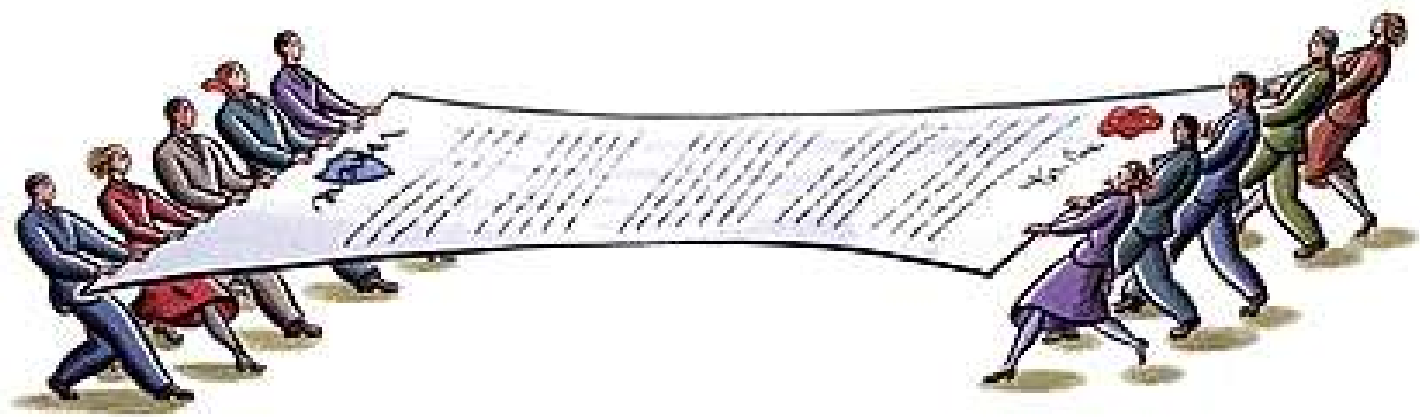
Devem ser criadas políticas para aplicação antes do contrato de pessoal.

- 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.

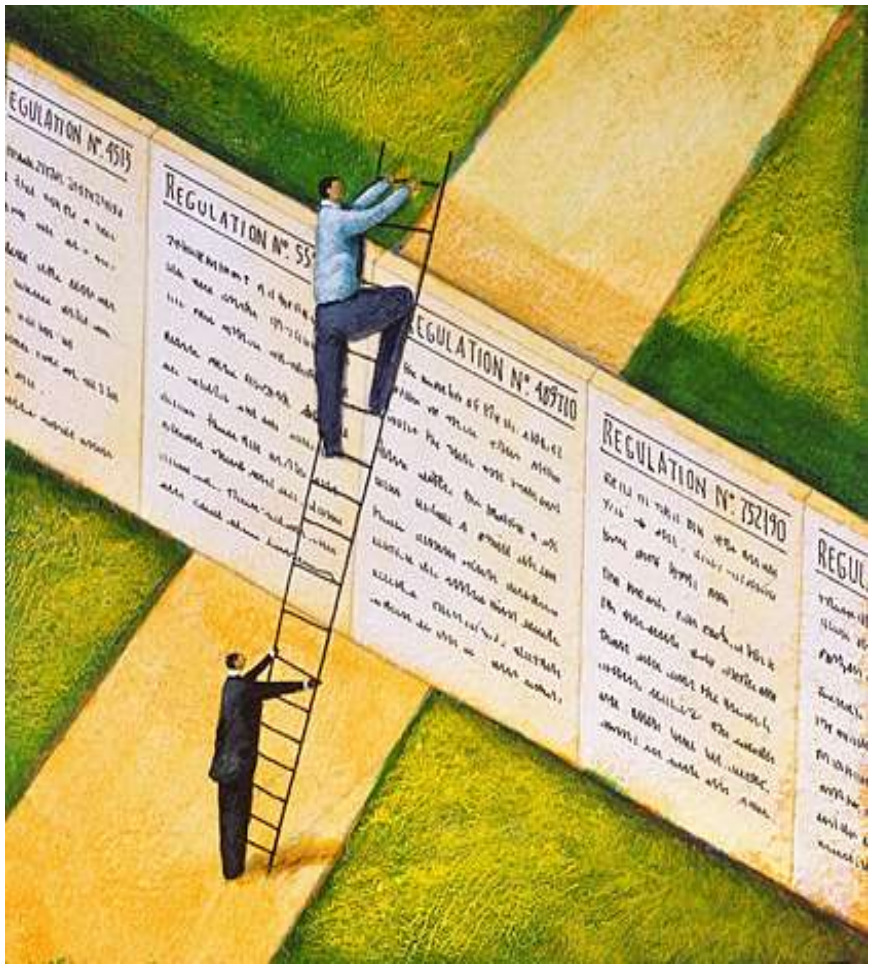


E políticas para aplicação no encerramento do contrato de pessoal.

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

Segurança física

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.

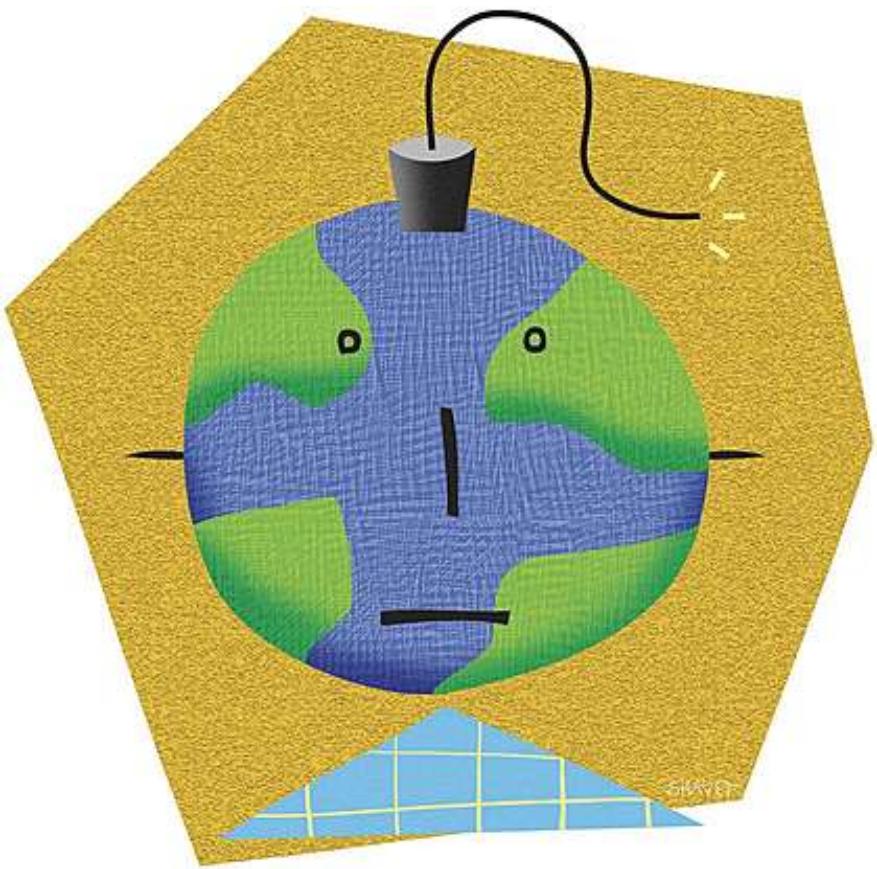
Segurança física

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:

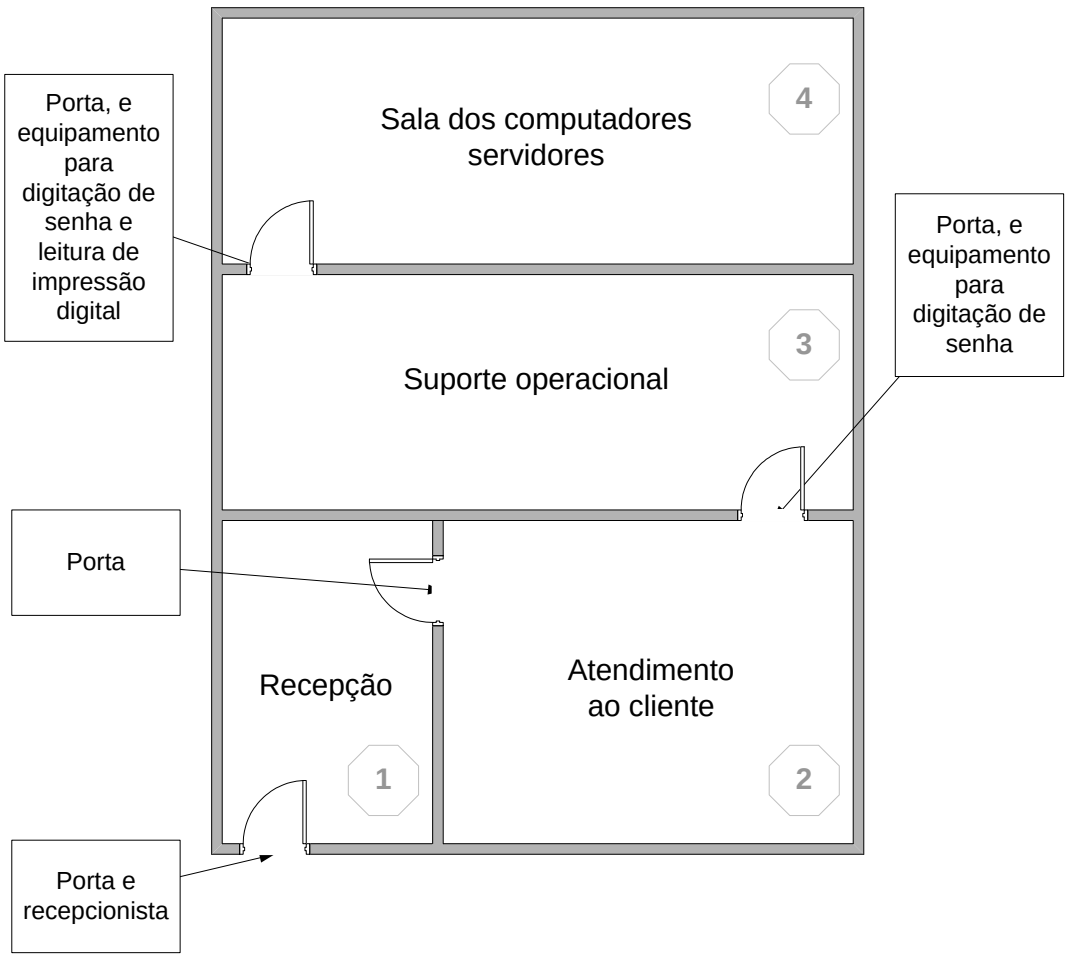
Naturais – Enchentes, tempestades, erupções vulcânicas, temperaturas extremas, alta umidade...

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.

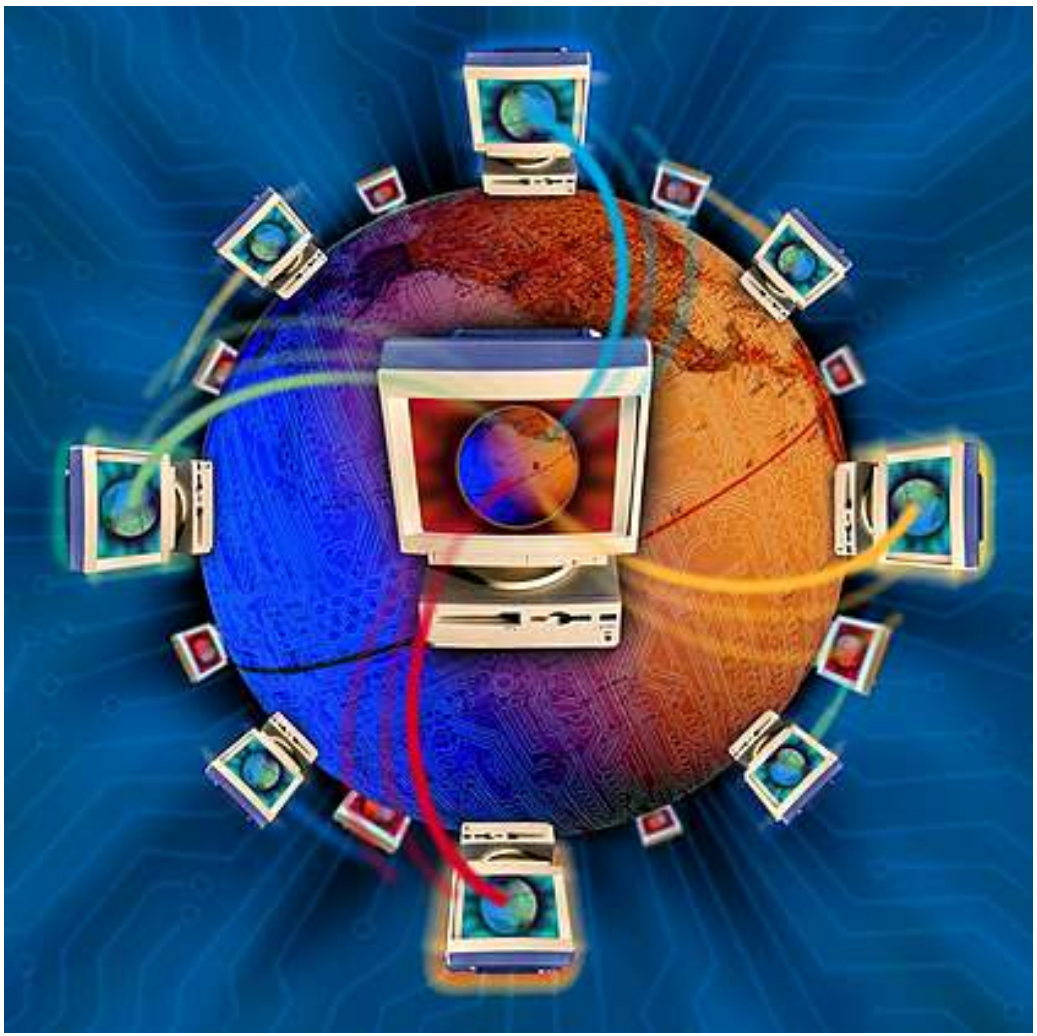
Segurança física

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.

Gestão das operações de TI

Gestão das operações de TI



As operações de TI envolve o controle sobre o hardware, mídias, gestão de privilégios, rede, segurança Internet, métodos de transmissão de informações, entre outros.

O objetivo é garantir o CID em todas estas operações.

Políticas devem ser criadas para este fim.

Gestão das operações de TI

As responsabilidades operacionais devem ser atribuídas, e procedimentos precisam ser escritos, aprovados e publicados.

Gestão das operações de TI

Os serviços operacionais de tecnologia da informação prestados por terceiros precisam ser regulados e devidamente gerenciados.

Gestão das operações de TI

A necessidade de sistemas precisa ser planejada de acordo com as necessidades demonstradas nos processos de negócio.

Estes sistemas devem passar por avaliação e homologação antes da entrada definitiva em operação.

Gestão das operações de TI

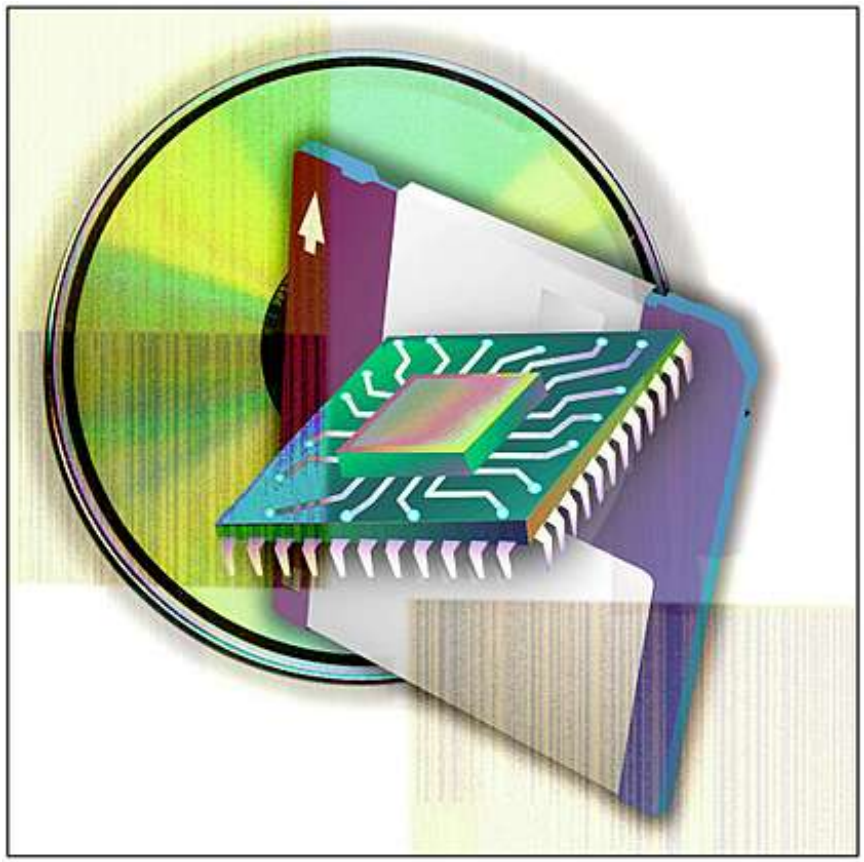
Uma política de cópia de segurança (backup) deve ser estabelecida.

As operações de backup precisam ser gerenciadas.

Gestão das operações de TI

A segurança das operações em rede é um importante fator a ser considerado na política de segurança da informação.

Gestão das operações de TI



Uma política para manuseio de mídias deve ser elaborada.

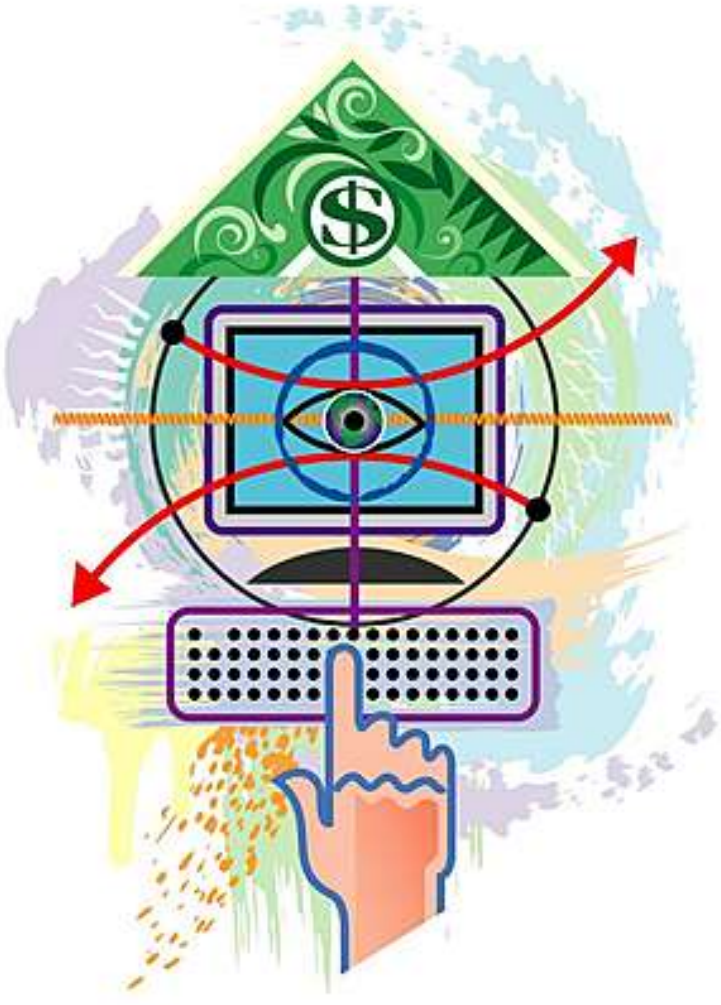
Questões tais como o gerenciamento, o descarte, procedimentos para tratamento da informação, e a segurança para os documentos de sistema, são importantes nesta política.

Gestão das operações de TI

A troca de informações deve ser considerada.

Questões importantes são: estabelecer procedimentos para troca de informações, mídias em trânsito, mensagens eletrônicas, sistemas de informações do negócio, entre outros.

Gestão das operações de TI



Por fim, é importante considerar o monitoramento de todas as operações em TI.

Para tanto, devem existir registros de auditoria, monitoramento do uso dos sistemas, proteção das informações de registro (log), registro de log tanto de operador quanto de administrador, registro em log das falhas, e mecanismo de sincronização dos relógios das máquinas.

Controle de acesso lógico

Controle de acesso lógico

É preciso elaborar uma política de controle de acesso, que apontará para os requisitos de negócio e para as regras de 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.

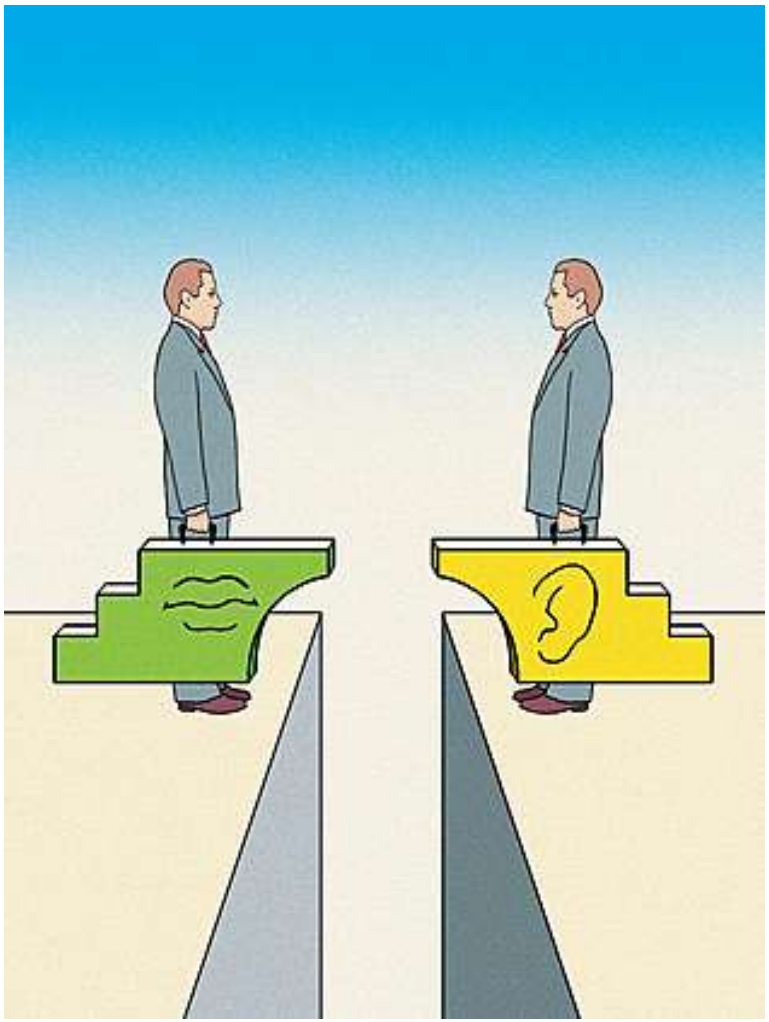
Controle de acesso lógico

O conceito de controle de acesso baseia-se em dois princípios:

1 – Separação de responsabilidades;

2 – Privilégios mínimos.

Controle de acesso lógico



O conceito de separação de responsabilidades implica na separação de um determinado processo de modo que cada parte possa ser realizada por uma pessoa diferente.

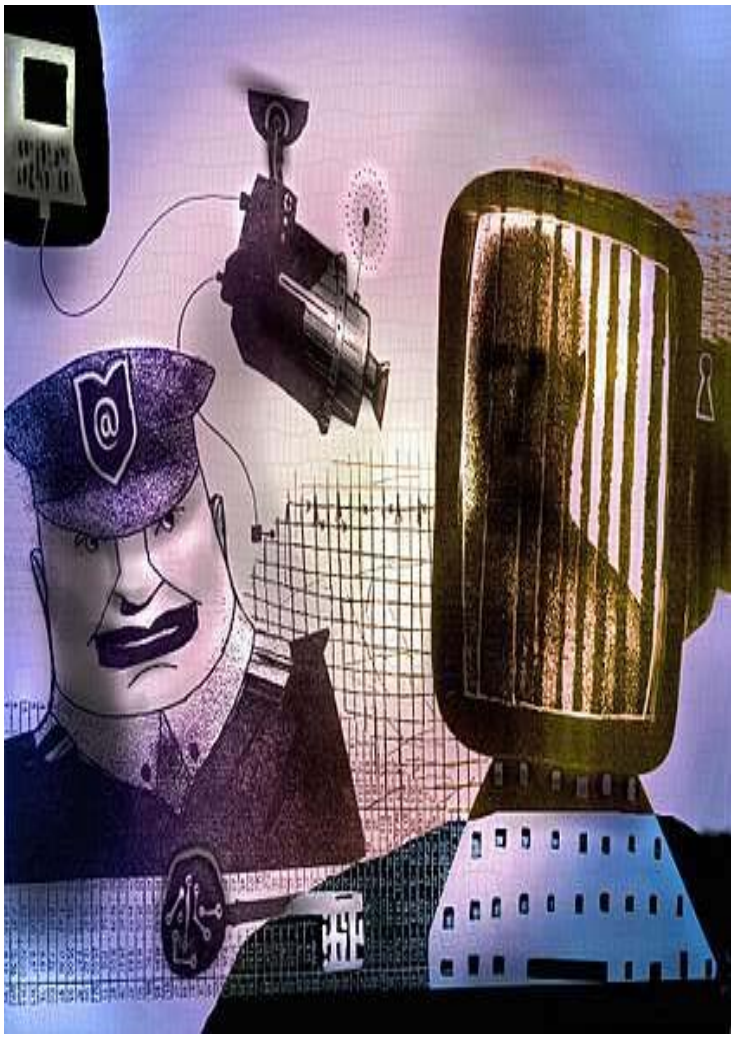
Isto obriga os colaboradores a interagir para concluir um determinado processo, diminuindo as chances de fraudes.

Controle de acesso lógico

O conceito de privilégio mínimo implica na concessão apenas dos privilégios mínimos necessários para que uma pessoa realize suas atividades.

Isto evita o conhecimento de outras possibilidades, que eventualmente poderiam levar a incidentes de segurança da informação. Há um termo em inglês para este conceito: "*need-to-know*".

Controle de acesso lógico



A política de controle de acesso deve abranger pelo menos os seguintes temas:

1 – Definição dos requisitos de negócio para controle de acesso;

2 – Gerenciamento dos acessos pelos usuários;

3 – Definição das responsabilidades dos usuários;

4 – Controle de acesso à rede;

5 – Controle de acesso ao sistema operacional;

6 – Controle de acesso aos sistemas de informação;

7 – Computação móvel e trabalho remoto.

Desenvolvimento e aquisição de sistemas

Aquisição, desenvolvimento e manutenção de sistemas

A segurança dos dados e informações em sistemas é um dos mais importantes objetivos de um sistema de segurança da informação.

Os procedimentos de desenvolvimento destes sistemas são uma questão vital para a segurança, para a manutenção do CID das informações.

A política de desenvolvimento de sistemas é o mecanismos para garantir estes resultados.

Aquisição, desenvolvimento e manutenção de sistemas

A aquisição de sistemas possibilita o surgimento de diversas vulnerabilidades.

A utilização de códigos abertos disponibilizados por comunidades é um dos perigos muitas vezes ignorados.

A política de sistemas precisa garantir a diminuição destas vulnerabilidades.

Aquisição, desenvolvimento e manutenção de sistemas

O desenvolvimento e manutenção de sistemas também contém diversas vulnerabilidades.

Se não houver uma política explicita que oriente este desenvolvimento, vulnerabilidades poderão ser introduzidas no levantamento de requisitos, na construção do projeto, e na implantação do sistema.

Aquisição, desenvolvimento e manutenção de sistemas

A política de sistemas de informação deve se preocupar com os seguintes assuntos:

1 - Definição dos requisitos de segurança para sistemas;

2 – Processamento correto nas aplicações;

3 – Controles criptográficos;

4 - Segurança dos arquivos de sistema;

5 – Segurança nos processos de desenvolvimento e manutenção;

6 – Gestão das vulnerabilidades técnicas.

Gestão de incidentes de segurança

Gestão dos incidentes de segurança da informação

Apesar de todos os controles implementados, eventualmente ocorrerão incidentes de segurança da informação.

Estes incidentes podem ser uma indicação de que alguns dos controles não estão sendo eficazes, e este é um bom motivo para reavaliar os mesmos.

Gestão dos incidentes de segurança da informação

A política de segurança da informação deve se preocupar com pelo menos os seguintes assuntos sobre gestão de incidentes:

1 – Notificação e registro dos incidentes;

2 – Tratamento dos incidentes e melhoria contínua.

Plano de continuidade de negócio

Plano de continuidade do negócio (PCN)

O plano de continuidade de negócio é de fato uma política para que os negócios da organização não sejam interrompidos por incidentes de segurança da informação.

Isto significa que esta política deve garantir a existência de procedimentos de preparação, teste, e manutenção de ações específicas para proteger os processos críticos do negócio.

Um PCN é constituído de 5 fases.

Plano de continuidade do negócio (PCN)

1 - Iniciação e gestão do projeto.

Nesta fase são estabelecidos o gerente e a equipe do projeto, que elaboram o plano deste projeto.

Plano de continuidade do negócio (PCN)

2 - Análise de impacto para o negócio.

Nesta fase são identificados os tempos críticos dos processos essenciais da organização, e determinados os tempos máximos de tolerância de parada para estes processos (*downtime*).

Plano de continuidade do negócio (PCN)

3 – Estratégias de recuperação.

Nesta fase são identificadas e selecionadas as alternativas adequadas de recuperação para cada tipo de incidente, respeitando os tempos definidos na etapa anterior (análise de impacto para o negócio).

Plano de continuidade do negócio (PCN)

4 – Elaboração dos planos.

Nesta fase são construídos os documentos, os planos de continuidade propriamente ditos. Estes documentos são resultados da *análise de impacto para o negócio*, e *estratégias de recuperação*.

Plano de continuidade do negócio (PCN)

5 – Teste, manutenção e treinamento.

Nesta fase são estabelecidos os processos para teste 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.

Conformidade com os aspectos legais

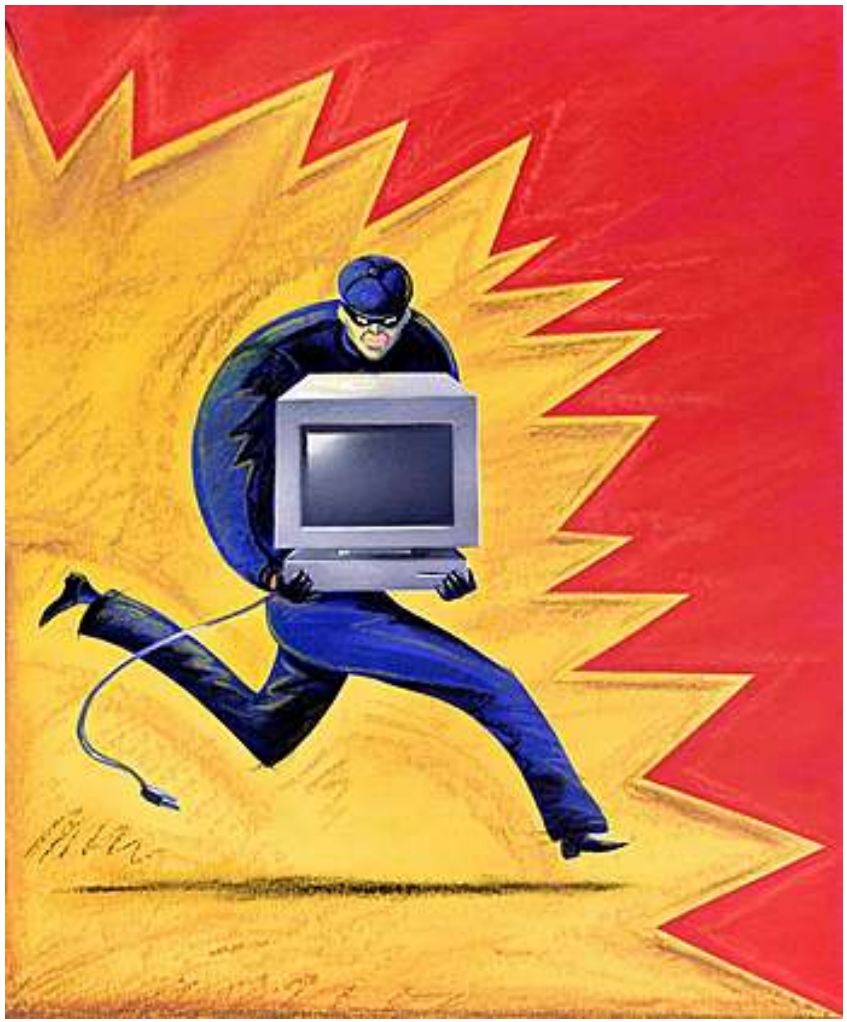
Conformidade com os aspectos legais

Todo o sistema de segurança da informação, com todos os seus controles, deve estar em plena harmonia e conformidade com as leis internacionais, nacionais, estaduais, municipais, e com as eventuais regulamentações internas da organização, bem como com as orientações de normatização e regulamentação do mercado.

Conformidade com os aspectos legais

A política de segurança precisa garantir que seja avaliada a legislação vigente, que existam mecanismos para determinar se um crime envolvendo sistemas e computadores foi cometido, e que estes procedimentos possibilitem a preservação e coleta das evidências incriminatórias.

Conformidade com os 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.

Conformidade com os aspectos legais

Mas como os crimes podem envolver computadores?

Crime apoiado por computador. Fraudes, pornografia infantil, etc.

Crime específico de computador. DOS, sniffers, roubo de senhas, etc.

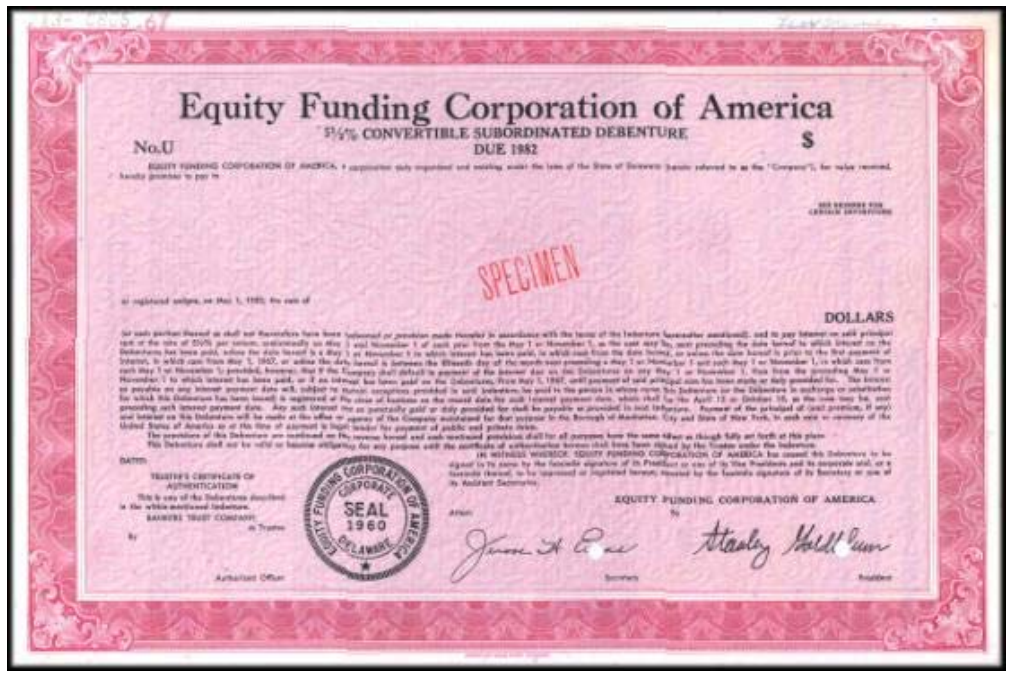
Crimes em que o computador é um mero elemento. Lista de clientes de traficantes, etc.

Vejamos alguns incidentes históricos..

Conformidade com os aspectos legais

Equity Funding. Considerado o primeiro crime grande envolvendo computadores. A organização usou seus computadores para criar falsos registros e outros instrumentos para aumentar o valor da organização no mercado.

Os auditores, que checavam todas as evidencias nos computadores ao invés de avaliar as transações reais, foram enganados por muito tempo.


Equity Funding Corporation of America

5½% CONVERTIBLE SUBORDINATED DEBENTURE DUE 1982

No.U $

SPECIMEN

DOLLARS

SEAL 1960

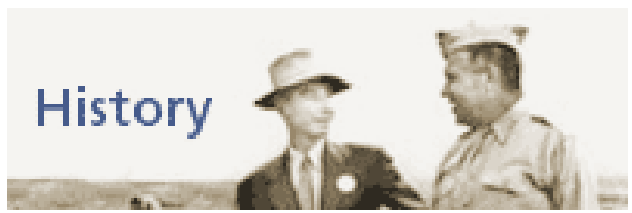
EQUITY FUNDING CORPORATION OF AMERICA

Conformidade com os aspectos legais

412 Gang. Em 1982 um grupo auto-intitulado “412 Gang” ganhou fama nacional nos Estados Unidos quando derrubou o servidor de banco de dados do “Memorial Sloan Kettering Cancer Center”, e depois invadiu os computadores de uma organização militar chamada “Los Alamos”, no Novo México.

MEMORIAL SLOAN-KETTERING CANCER CENTER

Los Alamos NATIONAL LABORATORY EST. 1943



Conformidade com os aspectos legais

Kevin Mitnick. Sem dúvida, trata-se do mais famoso e reconhecido hacker de todos os tempos. Foi o mestre na arte da engenharia social, técnica que empregou extensivamente para obter acesso a muitos sistemas de computores.

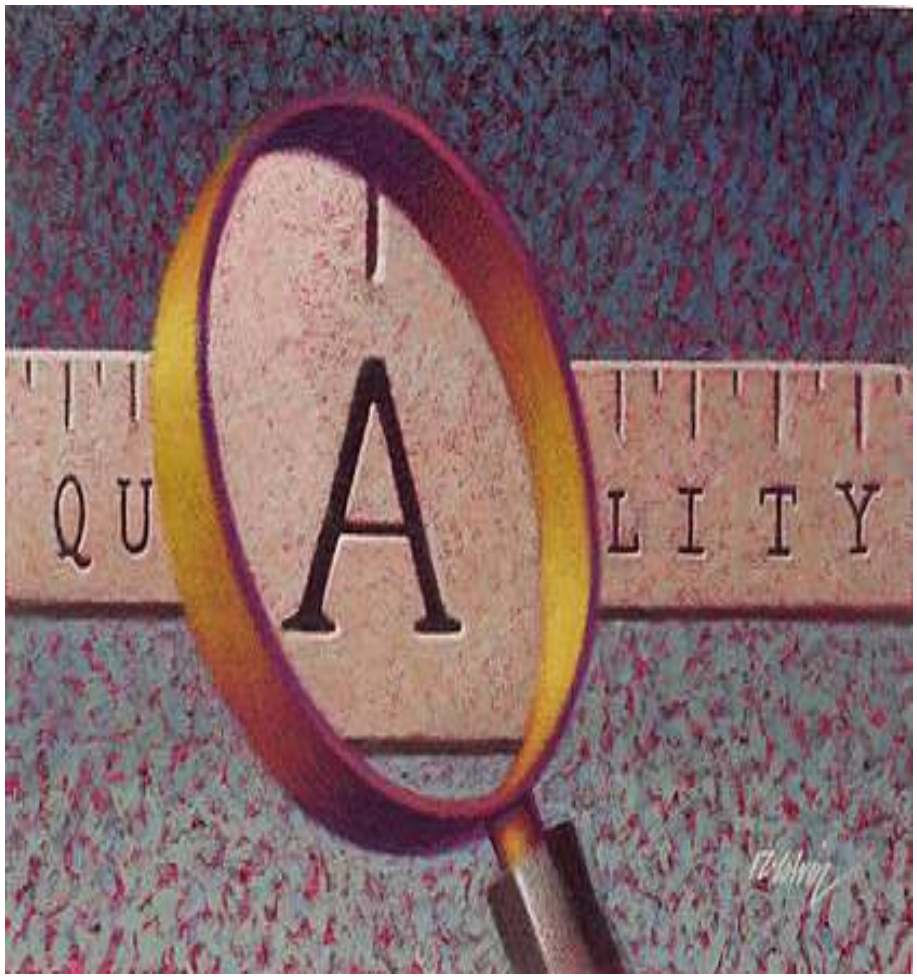
Hoje ele presta serviços de segurança da informação, e seu site é o www.kevinmitnick.com.

Conformidade com os aspectos legais

A política de segurança deve garantir procedimentos para identificação e adequação à legislação vigente.

Isto inclui os direitos de propriedade intelectual, a proteção aos registros organizacionais, a proteção de dados e privacidade de informações pessoais, a prevenção de mau uso dos recursos de processamento da informação, e a regulamentação dos controles de criptografia.

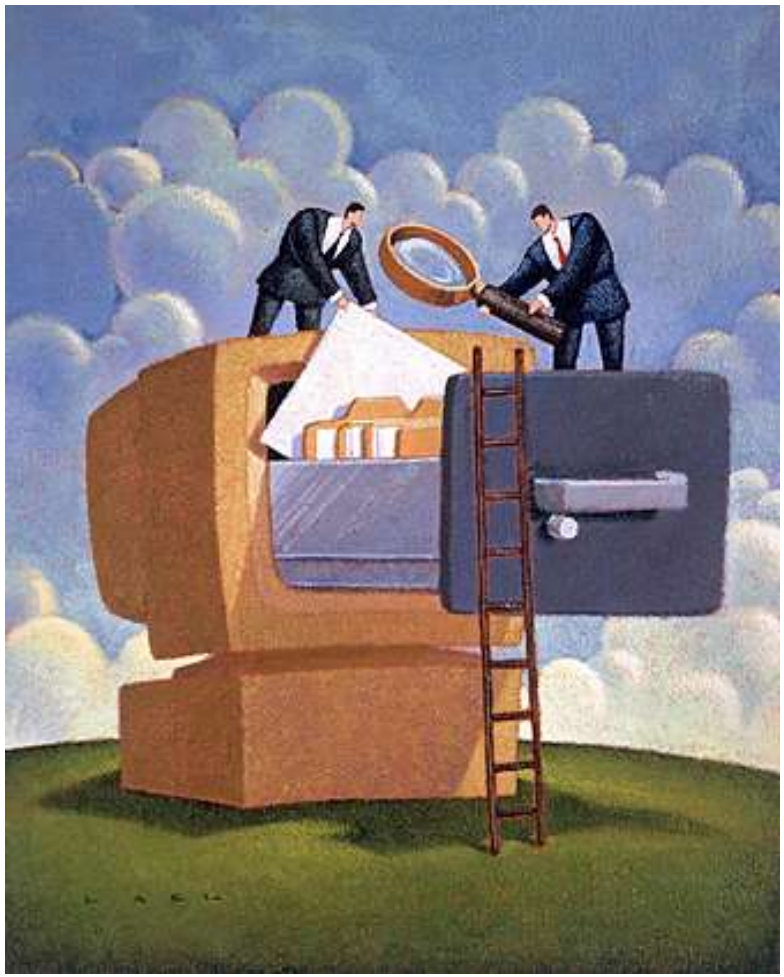
Conformidade com os aspectos legais



Conformidade entre as políticas de segurança da informação e também a conformidade técnica.

Isto significa que devem ser consideradas as políticas e normas de segurança, e a avaliação técnica destas normas.

Conformidade com os aspectos legais



E finalmente as questões referentes à auditoria.

A política deve garantir que existam controles de auditoria, e proteção às ferramentas de auditoria, o que garantirá a confiabilidade destas ferramentas.

Auditoria em Tecnologia da Informação

Fim