
Segurança Computacional

Segurança da Informação
Segurança de Redes
Segurança de Sistemas
Segurança de Aplicações

Símbolos

- Símbolos: S_1, S_2, \dots, S_n

Um símbolo é um sinal (algo que tem um caráter indicador) que tem uma determinada forma, portanto, sendo algo baseado num conceito puramente sintático (forma).

Exemplos: € H ħ O T ? ? - ?

Símbolos

- A princípio, nada é dito sobre eles próprios.
 - Tudo o que é assumido é que eles podem ser unicamente reconhecidos.
-

Dados

- Dado

Um símbolo, mas considerando-se algum significado.

Exemplos: ? ! % 5 = @ Ø

A informação de um símbolo

- Informação

Um **símbolo**, mas considerando o **significado** (semântica), **com relação a um contexto** no qual o símbolo está inserido.

Exemplos: ? ! % 5 = @ Ø

Alfabeto

- Um conjunto de símbolos.
 - Exemplo 1: O conjunto de símbolos, representando as letras do alfabeto da língua inglesa ou da língua portuguesa.
-

Alfabeto

Exemplo 2:

O conjunto dos símbolos que representam os algarismos usados no sistema de numeração romano.

Alfabeto

Exemplo 3:

O conjunto dos símbolos que representam os algarismos usados nos sistemas de numeração binário, decimal ou hexadecimal.

Cadeias de Símbolos

- **Sequências de símbolos** de um alfabeto: S_1, S_2, \dots, S_n
 - $S_1 S_2 S_3 S_4 \dots S_n$ (cadeias, strings)
 - palavras, números, códigos, ...
-

Cadeias de Símbolos

- Essas cadeias de símbolos, inseridas num determinado contexto, proporcionam alguma informação relevante a ser considerada.
-

Terminologia

- Existem certas palavras usadas nas terminologias da Teoria da Informação ou na terminologia dos Sistemas de Informação, tais como:

“informação”, “transmissão”,
“codificação”, “decodificação”

Terminologia

- Mas, um exame mais minucioso revelará que tudo o que é realmente assumido é uma **fonte de informação**, ou seja, uma **sequência de símbolos** S_1, S_2, \dots, S_n de um alfabeto.
-

Fontes de Informação

Na forma **alfabética convencional**:

- Um livro.
 - Uma notícia formal impressa.
 - Um relatório financeiro de uma empresa.
-

Fontes de Informação

Em forma **não alfabética convencional**:

- Uma dança.
 - Uma música.
 - Uma equação matemática.
 - Outras atividades humanas, com várias formas de símbolos para representar sua informação.
-

Fontes de Informação

- **Informação** também existe em forma contínua.
 - A **natureza**, geralmente, **supre informação** nessa forma.
-

Fonte de Informação

- A prática moderna é amostrar o sinal contínuo em intervalos de tempo espaçados igualmente, e então digitalizar a quantidade observada (**codificação**).
 - A **informação** pode, então, ser **transmitida** como um *stream* de dígitos binários.
-

Recursos da Informação

- Arquivos.
 - Objetos.
 - Banco de dados.
-

Valor da Informação

- Muitos **recursos de informação** que são disponíveis e mantidos em sistemas de informação distribuídos através de redes, têm um alto valor intrínseco para seus usuários.
 - Toda informação tem valor e precisa ser protegida contra **acidentes** ou **ataques**.
-

Segurança da Informação

- Processo de proteção de informações:
 - **armazenadas em computadores** situados em **redes**;
 - **transportadas sobre essas**, através de canais de comunicação e dos mais diversos elementos de rede.
-

Problemas de Segurança da Informação

- Garantir que pessoas mal intencionadas não leiam ou, pior ainda, modifiquem mensagens enviadas a outros destinatários.
-

Problemas de Segurança da Informação

- Pessoas que tentam ter acesso a serviços remotos, os quais elas não estão autorizadas.
 - Distinção entre uma mensagem supostamente verdadeira e uma mensagem falsa.
-

Problemas de Segurança da Informação

- Mensagens legítimas podem ser capturadas e reproduzidas.
 - Pessoas que negam ter enviado determinadas mensagens.
-

Soluções de Segurança da Informação

- Armazenadas em computadores situados em rede:
(arquivos, aplicações em rede, bancos de dados e sistemas operacionais)
 - Soluções: Criptografia,
Segurança de Sistemas,
Segurança de Aplicações.
-

Soluções de Segurança da Informação

- Transportadas sobre redes:
 - através de canais de comunicação, dos mais diversos elementos de rede e protocolos.
 - **Criptografia** (codificação e decodificação da informação transportada).
 - **Segurança de Rede**.
-

Segurança de Rede

- Tornar seguro os **serviços** providos numa **rede**, no sentido de:
-

Segurança de Rede

- Não permitir que um cliente e um servidor interajam diretamente;
 - Isolamento entre uma rede interna e uma rede externa.
-

Segurança de Rede

- Descobrir os pontos fracos, por onde se pode atacar numa rede.
 - Verificar quem está tentando entrar na rede, antes de revelar informações sigilosas ou entrar numa transação.
-

Segurança de Rede

- Manter sigilo das informações que trafegam numa rede.
 - Certificar que uma mensagem recebida é legítima.
 - Provar o envio de uma mensagem.
-

Segurança de Rede

- Detectar intrusões numa rede.
 - Disfarçar os verdadeiros recursos da rede, visando o isolamento de um atacante.
-

Segurança de Sistemas

- Invasão por usuário:
 - Forma de acesso não autorizado a uma máquina, com aquisição da elevação de privilégios e execução de ações além daquelas autorizadas.
 - Invasão por intrusão.
-

Segurança de Sistemas

- Invasão por software:
 - Pode tomar a forma de um Vírus, um Cavalo de Tróia ou um Worm.
 - Invasão sem intrusão.
-

Segurança de Sistemas

- Análise dos sistemas para evidenciar o comprometimento.
 - Verificação de evidência de tentativas de invasão, através dos arquivos de log.
 - Busca de danos no sistema de arquivos.
-

Segurança de Sistemas

- Verificação da estabilidade e da disponibilidade do sistema.
 - Validação da operação do HW.
 - Garantia da estabilidade da energia.
-

Segurança de Sistemas

- Segurança no acesso à rede: desativar serviços desnecessários.
 - Retirada da máquina da rede.
 - Identificação dos serviços necessários.
 - Identificação de dependências de serviços.
 - Configuração de serviços.
 - Retorno da máquina à rede.
-

Segurança de Sistemas

- Instalação de Firewalls.
 - Identificação das necessidades de proteção por Firewall.
 - Avaliação de Firewalls.
 - Configuração: regras de Firewall.
-

Segurança de Sistemas

- Segurança na acessibilidade do software.
 - Identificação dos softwares necessários.
 - Instalação dos softwares com segurança (origem confiável).
 - Determinação das dependências de software.
-

Segurança de Sistemas

- Preparando-se para o desastre.
 - Compreender a recuperação de desastres.
 - Documentos de alterações na configuração de servidores.
 - Preparação de re-instalação automática.
-

Segurança de Sistemas

- Segurança nos controles de acesso.
 - Permissões e propriedades de arquivos.
 - Listas de controle de acesso.
 - Controles de acesso de arquivos e diretórios.
-

Segurança de Sistemas

- Segurança no armazenamento de dados.
 - Procedimentos apropriados:
armazenamento seguro e remoção de cópias de dados em texto simples.
 - Criptografia de arquivos.
-

Segurança de Sistemas

- Segurança na autenticação do usuário.
 - Módulos PAM
(Pluggable Authentication Modules)
-

Segurança de Sistemas

- Ambientes de execução restrita.
 - Proteger a execução de serviços de rede, fornecendo o mínimo possível de funcionalidade a usuários externos.
 - Construção de ambientes restritos, através de comandos apropriados de SO.
-

Segurança de Sistemas

- Segurança nas comunicações.
 - Uso de SSH.
 - Criação de VPN.
 - IPSec
-

Segurança de Sistemas

- Instalar software de monitoramento de rede.
 - Analisador de rede.
 - Sistema de Detecção de Intrusão de Rede.
 - Honeypots.
-

Segurança de Sistemas

- **Arquivos de log.**
 - Podem dar uma idéia sobre o que as diferentes partes do sistema estão fazendo.
 - Podem oferecer perfis de atividades.
 - Proteção, Arquivamento (Backup).
 - Organização dos registros de logs.
 - Servidor centralizado.
 - Gerenciamento dos arquivos de log.
 - Pesquisa de arquivos de log.
-

Segurança de Sistemas

- Gerenciamento e Monitoramento de Patches.
 - Aplicar atualizações.
 - Testes de patches.
 - Gerenciamento de alterações.
-

Segurança de Sistemas

- Ferramentas de automonitoramento.
 - IDS de host: Tripwire, AIDE, AFICK, Radmin.
 - Verificado de senha: John the Ripper
 - Configuração do monitoramento de rede:
 - Nmap
 - Nessus
-

Segurança de Aplicações em Rede

- Categorias de segurança:
 - Autenticação
 - Autorização
 - Gerenciamento de sessões
 - Parâmetros de entrada
 - Criptografia
 - Entre cliente/servidor.
 - Entre servidores.
-

Segurança da Informação

- Define-se como o processo de proteção de informações armazenadas em computadores situados em redes.
-

Segurança da Informação

- Proteção de informações para que sejam mantidos os aspectos de:
 - confidencialidade,
 - Integridade,
 - disponibilidade.
-

Mercado

- Segurança voltada para o mercado corporativo: tecnologias avançadas com alta capacidade de tráfego e gerenciamento dos recursos de informação.
 - Segurança voltada para o mercado doméstico: usuário da Internet.
-

Segurança da Informação

- Porque ...

os sistemas computacionais ou de comunicação, que armazenam ou transmitem informação são vulneráveis (sujeito a intrusões).

O Conceito de Intrusão

- **Análise da Vulnerabilidade** (descobrir o melhor caminho para chegar até a invasão).
 - **Preparação das Ferramentas** (constrói ou escolhe as ferramentas para a invasão).
 - **Ameaça ou Tentativa** (quando o invasor pula o muro).
 - **Ataque** (concretiza o arrombamento).
 - **Invasão ou Penetração** (quando obtém sucesso).
-

Vulnerabilidade

- “Pontos Fracos”
 - Probabilidade de uma **ameaça** transformar-se em realidade.
 - Uma **falha de segurança** em um sistema de software ou de hardware que pode ser explorada para permitir a efetivação de uma **intrusão**.
-

Ameaça

- “Pulando o Muro”
 - Uma ação ou evento que pode prejudicar a segurança.
 - É a **tentativa de ataque** a um sistema de informação, explorando suas vulnerabilidades, no sentido de causar dano à **confidencialidade**, **integridade** ou **disponibilidade**.
-

Ataque

- “Arrombamento”
 - O ato de **tentar desviar dos controles de segurança** de um sistema.
 - Qualquer **ação que comprometa a segurança** da informação de propriedade de uma organização.
-

Ataques

- Pode ser **ativo**, tendo por resultado a **alteração dos dados**.
 - Pode ser **passivo**, tendo por resultado a obtenção da informação:
 - escuta oculta de transmissões.
 - análise de tráfego.
-

Ataques

- Pode ser **externo**, quando originado de fora da rede protegida.
 - Pode ser **interno**, quando originado de dentro da rede protegida.
-

Ataques

- O fato de um ataque estar acontecendo, não significa necessariamente que ele terá sucesso.
 - O nível de sucesso depende da vulnerabilidade do sistema ou da eficiência das contramedidas de segurança existentes.
-

Intrusão ou Invasão

- Sucesso no ataque.
 - Obtenção da Informação.
 - Acesso **bem sucedido**, porém não autorizado, em um sistema de informação.
-

Contramedidas

- Mecanismos ou procedimentos colocados num sistema para reduzir **riscos**.
 - **Riscos** são provenientes de vulnerabilidades, ameaças, e ocasionam impacto.
-

Risco

- Risco é a probabilidade da ocorrência de uma ameaça particular.
-

Análise de Risco

- **Análise de Risco** – Identificação e avaliação do risco que os recursos da informação estão sujeitos.
-

Gerenciamento de Riscos

- O processo total de identificar, de controlar e minimizar os riscos que podem afetar os recursos de informação do sistema.
-

Gerenciamento de Riscos

- Inclui a análise de risco, a análise de custo-benefício, a avaliação de segurança das proteções e a revisão total da segurança.
-

Risco Residual

- Riscos ainda existentes depois de terem sido aplicadas medidas de segurança.
-

Impacto

- É a representação (normalmente em forma de avaliação) do grau de dano percebido associado aos bens de uma empresa.
 - A consequência para uma organização da perda de **confidencialidade**, **disponibilidade** e (ou) **integridade** de uma informação.
-

Impacto

- O impacto deve ser analisado quanto à modificação, destruição, divulgação ou negação de informação.
 - Relaciona-se a imagem da empresa, ao dano, a perdas financeiras ou legais e a outros problemas que podem ocorrer como consequência de uma ruptura da segurança.
-

Segurança da Informação

- De uma forma mais simplificada:
 - Proteção de informações para que sejam mantidos os requisitos de:
 - confidencialidade,
 - integridade,
 - disponibilidade.
-

Segurança da Informação

- Segurança da Informação trata de garantir a existência dos requisitos fundamentais para proporcionar um nível aceitável de segurança nos recursos de informação.
-

Segurança da Informação

- Definir restrições aos recursos da informação.
 - Segurança da Informação é a gestão de tais restrições.
 - Para gerir restrições é preciso definir políticas de segurança.
 - Um conjunto de políticas de segurança define um Modelo de Segurança.
-

Os Requisitos de Segurança

- Disponibilidade
 - Confidencialidade
 - Privacidade (**)
 - Integridade
 - Autenticidade
 - Controle de Acesso
 - Não-Repúdio da Informação
-

Disponibilidade (Availability)

- É o requisito de segurança em que a informação deve ser entregue para a pessoa certa, no momento que ela precisar.
 - A informação estará disponível para acesso no momento desejado.
 - Proteção contra interferência no meio para acessar os recursos.
-

Confidencialidade

- É o requisito de segurança que visa a proteção contra a revelação de informação a indivíduos não autorizados.
 - Garante que a informação em um sistema, ou a informação transmitida são acessíveis somente a partes autorizadas.
-

Privacidade (Privacy)

- É o requisito de segurança em que a informação pode ser fornecida, mas somente com a autorização do proprietário da informação.
 - Informações médicas ou financeiras.
 - Diz respeito ao que é pessoal.
-

Integridade

- É o requisito de segurança que visa a proteção da informação contra modificações não autorizadas.
 - Garante que somente partes autorizadas podem modificar a informação.
 - Modificação inclui: escrever, mudar, mudar status, apagar, criar e atrasar ou responder mensagens.
-

Autenticidade

- É o requisito de segurança que visa validar a identidade de um usuário, dispositivo, ou outra entidade em um sistema, frequentemente como um pré-requisito a permitir o acesso aos recursos de informação no sistema.
-

Autenticidade

- Garante que a origem da informação é corretamente identificada, assegurando que a identidade não é falsa.
-

Acesso

- **Interação** entre um usuário e o sistema que permite a informação fluir de um para o outro.
-

Controle de Acesso

- Procedimentos operacionais para detectar e prevenir acessos não autorizados e permitir acessos autorizados num sistema.
-

Não-Repúdio

- Requer que nem o transmissor nem o receptor da informação, possam negar o envio da informação.
 - O sistema **não permite a negação**, por parte do usuário, do envio de determinada informação.
-

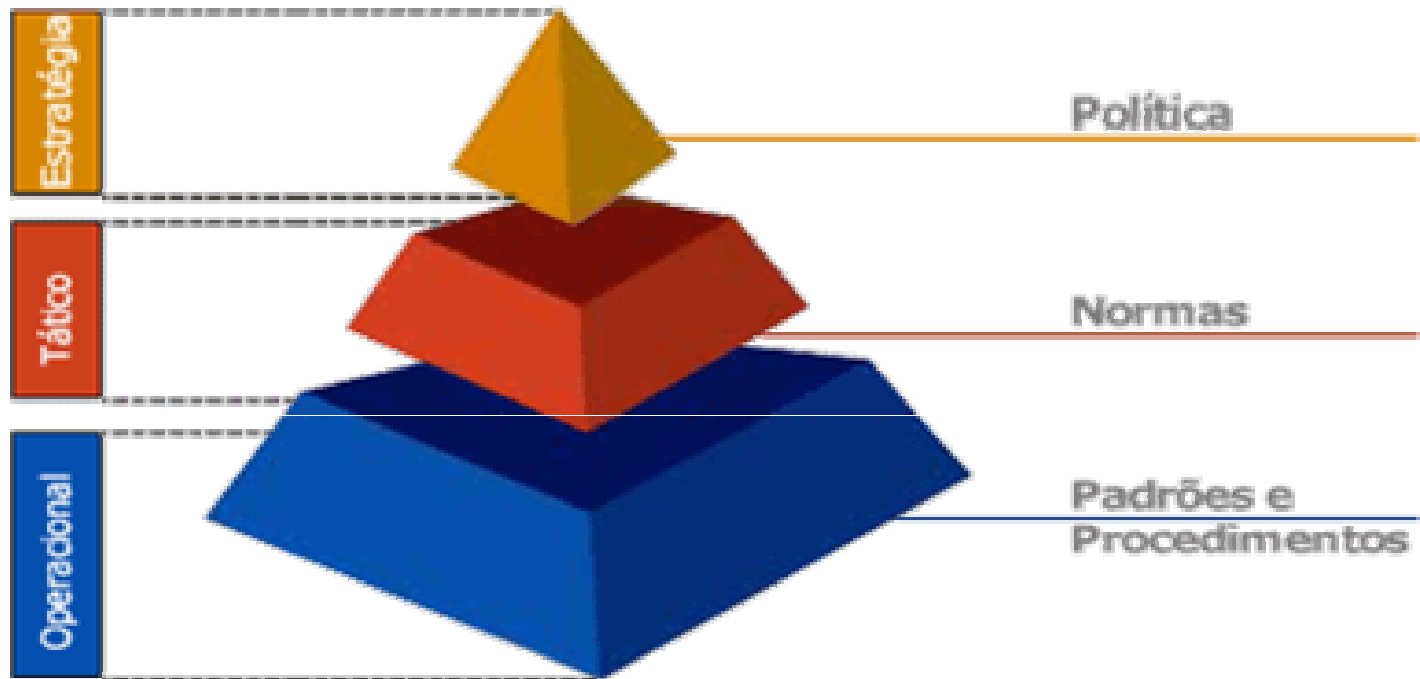
Estudo de Caso:

Segurança da Informação no
Bradesco

O que é Segurança da Informação

- A segurança da informação é um conjunto de medidas que se constituem basicamente de controles e política de segurança, tendo como objetivo a proteção das informações dos clientes e da empresa, controlando o **risco de revelação** ou **alteração por pessoas não autorizadas**.
-

Níveis de Segurança da Informação



Nível de Estratégia

Estratégia

É o nível que refere-se às Políticas da Organização e descreve "o que deve ser feito".

Nível Tático

Tático

É o nível que refere-se às Normas da Organização e com base nas Políticas, descreve as "regras" a serem adotadas.

Nível Operacional

Operacional

É o nível dos Procedimentos da Organização e com base nas Normas, descreve "como serão implementadas as regras".

Política de Segurança (Exemplo BRADESCO)

- Política de Segurança é um conjunto de diretrizes que definem formalmente as regras e os direitos dos funcionários e prestadores de serviços, visando à proteção adequada dos ativos da informação.
-

Base da Política (Exemplo BRADESCO)

- Essa política está baseada em diretrizes de segurança e diretivas de privacidade.
-

Diretrizes de Segurança (Exemplo do BRADESCO)

- Proteger as informações
 - Assegurar Recursos
 - Garantir Proteção
 - Garantir Continuidade
 - Cumprir Normas
 - Atender às Leis
 - Selecionar Mecanismos
 - Comunicar Descumprimento
-

Diretivas de Privacidade (Exemplo BRADESCO)

- O Banco Bradesco esclarece como as informações dos clientes são armazenadas em seus computadores, garantindo: confidencialidade, integridade e disponibilidade.
-

Confidencialidade: Propriedade de manter a informação a salvo de acesso e divulgação não autorizados.

Disponibilidade: Propriedade de manter a informação disponível para usuários, quando estes dela necessitarem.

Integridade: Propriedade de manter a informação
acurada, completa e atualizada.

Diretivas de Privacidade - Bradesco

- **As informações de nossos clientes seguem as seguintes diretivas:**
 - ❑ As informações são coletadas de forma legal e sob o conhecimento do usuário;
 - ❑ As informações são enviadas ao Bradesco de forma segura com métodos de criptografia e certificação digital;
 - ❑ As informações enviadas ao Bradesco serão armazenadas de forma íntegra, sem alteração de qualquer parte;
-

Diretivas de Privacidade - Bradesco

- As informações são armazenadas de forma segura e criptografada restringindo o acesso somente às pessoas autorizadas;
 - As informações serão utilizadas apenas para as finalidades aprovadas pela Organização;
 - As informações dos clientes nunca serão fornecidas a terceiros, exceto por determinação legal ou judicial.
-

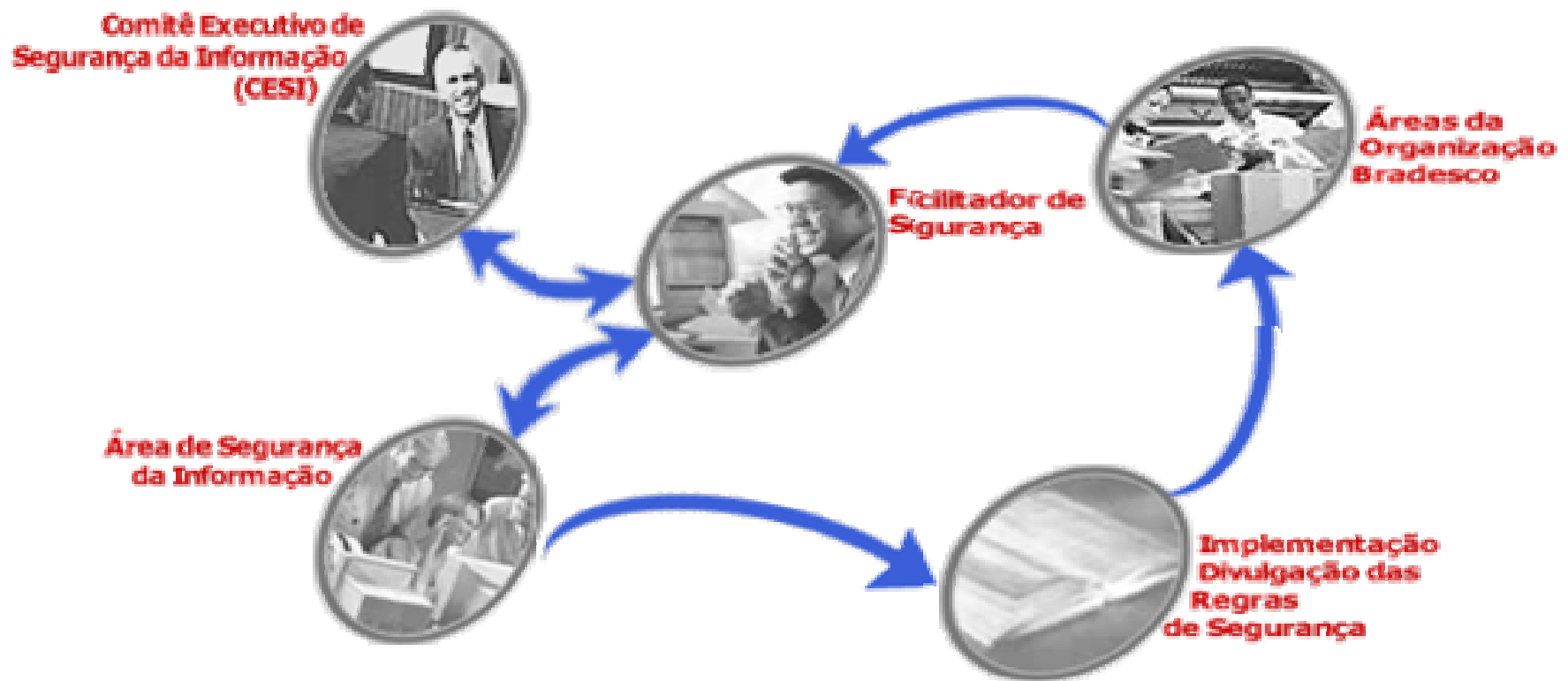
Processo de Segurança e Acompanhamento (BRADESCO)

- O processo de segurança da informação pode ser melhor ilustrado, conforme o ciclo abaixo:
-



Organização da Segurança (BRADESCO)

- A Organização Bradesco definiu uma estrutura formal, com objetivos e responsabilidades específicas, para tratar da segurança da informação de uma forma adequada.
 - O objetivo dessa estrutura é definir, manter e melhorar a segurança da informação no ambiente da Organização Bradesco.
-



Infra-estrutura de Segurança da Informação (1)

O **projeto de segurança** da informação pode ser definido como segue:

- **Análise de riscos.**
 - Criação de uma **política de segurança corporativa.**
 - Processo de **conscientização do pessoal** de informática e demais usuários.
 - Proteção contra **softwares maliciosos.**
-

Infra Estrutura de Segurança da Informação (2)

- **Firewall e Hosts de Segurança;**
 - Sistemas de **Criptografia (Protocolos de Segurança).**
 - Sistemas de **Detecção de Intrusão.**
 - Sistemas de **Análise de Vulnerabilidades.**
 - Ferramentas de **Autenticação** de Usuários: **assinaturas digitais, certificação digital.**
 - Procedimentos de **Auditoria.**
 - **Aspectos Jurídicos .**
-