Relação entre: Dados, Informação e Conhecimento

Dados	Informações	Conhecimento
Simples observações sobre o estado do mundo	Dados dotados de relevância e propósito	Informação valiosa da mente humana
• Facilmente estruturado • Facilmente obtido por máquinas • Frequentemente quantificado • Facilmente transferível	• Requer unidade de análise • Exige consenso em relação ao significado • Exige necessariamente a medição humana	• De difícil estruturação • De difícil captura em máquinas • Frequentemente tácito • De difícil transferência

As empresas já perceberam que o domínio da tecnologia como aliado para o controle da informação é vital.

O controle da informação é um fator de sucesso crítico para os negócios e sempre teve fundamental importância para as corporações do ponto de vista estratégico e empresarial (SYNNATT, W. R. *The Information Weapon – Winning Customers and Markets with Tecnhonology*. Ed.John Wiley & Sons, 1987; Feliciano Neto, Furlan e Higo, 1988 FELICIANO NETO, A. FURLAN, J. D. e HIGO, W. Engenharia da Informação – Metodologia, Técnicas e Ferramentas. Ed.McGraw- Hill. São Paulo, 1988).

Dispor da informação correta, na hora adequada, significa tomar uma decisão de forma ágil e eficiente. Com a evolução dos dados e sistemas, a informação ganhou mobilidade, inteligência e real capacidade de gestão. A informação é substrato da inteligência competitiva; deve ser administrada em seus particulares, diferenciada e salvaguardada.

1.2 O VALOR DA INFORMAÇÃO

O valor da informação está diretamente ligado à forma como auxilia os tomadores de decisão, dentro das organizações, a atingirem seus objetivos. Em outras palavras, o valor da informação poderia ser medido pelo grau de contribuição que a informação dá ao tempo de tomada de uma decisão ou ao aumento de lucros, por exemplo, provenientes dela.

Em linhas gerais, tanto mais valor terá uma informação quanto menor for o grau de incerteza que ela propicia à tomada de decisões. Imaginando-se uma decisão de compra, por exemplo, quanto mais informações se têm acerca das opções, seus custos e seus benefícios, melhor tende a ser a escolha de uma opção. Assim, quanto maior o valor atribuído a uma informação, maior qualidade ela trará ao processo decisório.

A informação, nos dias de hoje, tem um valor altamente significativo e pode representar grande poder para quem a possui, seja pessoa ou instituição. Seu valor é percebido à medida que vai se tornando presente em todas as atividades que envolvem pessoas, processos, sistemas, recursos financeiros, tecnologias, entre outros.

Ao longo da vida de uma pessoa, ou de uma organização, são coletadas e apreendidas diversas informações, que, mediante um processo sistemático, podem ser muito valorizadas, por exemplo, em uma empresa, informações de histórico de vendas, perfil de clientes, produtos mais vendidos são fundamentais. É importante destacar que apenas o acúmulo de informação não gera valor, é necessário que haja tais processos sistemáticos para que seu valor seja percebido e extraído.

Para que a informação seja valorizada na organização, é necessário um processo contínuo que deve cumprir algumas fases e passos lógicos, segundo Weitzen (1991).

Estes passos podem ser assim distribuídos:

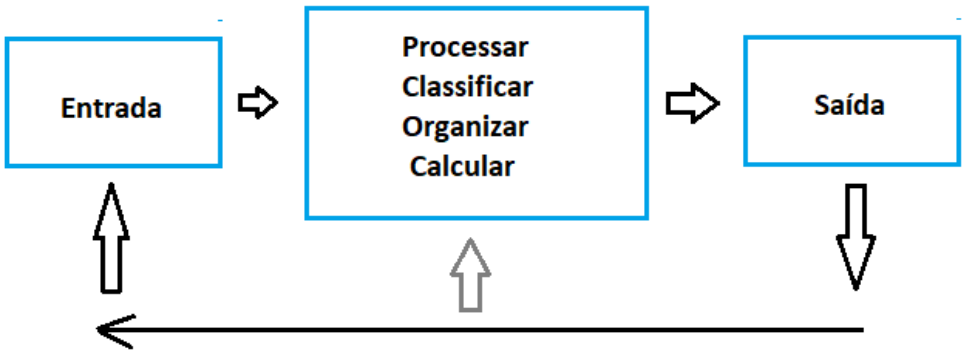
- Conhecer muitas informações;
- Aprender sobre as informações;
- Juntar e guardar as informações úteis;
- Selecionar, analisar e filtrar as informações de valor;
- Organizar as informações de forma lógica;
- Valorizar as informações (detalhes);
- Disponibilizar e usar as informações.

2 SISTEMAS DE INFORMAÇÃO

Um Sistema de Informação pode ser definido tecnicamente como um conjunto de componentes interrelacionados que coleta (ou recupera), processa, armazena e distribui informações destinadas a apoiar a tomada de decisões, a coordenação e o controle de uma organização.

Além de dar suporte à tomada de decisões, à coordenação e ao controle, esses sistemas também auxiliam os gerentes e trabalhadores a analisar problemas, visualizar assuntos complexos e criar novos produtos.

São três atividades em um sistema de informação que produzem as informações de que as organizações necessitam para: tomar decisões, controlar operações, analisar problemas e criar novos produtos ou serviços.



O Sistema de Informação contém informações sobre uma organização e sobre o ambiente que a cerca. As atividades básicas: Entrada, Processamento e Saída, produzem as informações de que as organizações necessitam.

O *Feedback* é a saída que volta a determinadas pessoas e atividades da organização para análise e refino da entrada. Aditivamente os Fatores Ambientais, tais como: clientes, fornecedores, concorrentes, acionistas e agências reguladoras integram a organização e seus sistemas de informação.

Em um caixa de supermercado:

Por exemplo, são registrados milhões de dados, como códigos de barras de produtos, preço e quantidade de cada item vendido.

De forma sintética, pode-se colocar que:

A **entrada** captura ou coleta dados brutos a partir de dentro da organização ou de seu ambiente externo.

O **processamento** converte esses dados brutos em uma forma significativa.

A **saída** transfere as informações processadas às pessoas, que as utilizarão, ou às atividades em que serão empregadas.

Os sistemas de informação também requerem um *feedback*, que é a entrada que volta a determinados membros da organização para ajudá-los a avaliar ou corrigir o estágio de entrada.

Sob uma perspectiva ampliada, os sistemas de informação compõem-se de:

- **Programas de Computador** (software) inter-relacionados entre si e entre os bancos de dados que eles tratam, compondo assim um sistema;
- **Materiais Tecnológicos** (hardware) itens de hardware como computadores, redes de computadores e dispositivos auxiliares, como periféricos, itens de comunicação de dados etc.;
- **Bancos de Dados ou Repositórios das Informações** que são tratadas pelo sistema;
- **Manuais e Procedimentos** relacionados com a correta operação do sistema e com o fluxo das informações por ele tratadas;
- **Recursos Humanos (*peopleware*)** habilitados a usarem o sistema de maneira eficiente e segura.

Em uma visão empresarial, o sistema de informação deve constituir uma solução baseada em recursos de tecnologia da informação, que integre com o composto organizacional e administrativo, capaz de enfrentar o desafio proposto pelo ambiente.

2.3 Ciclo de Vida da Informação

O Ciclo de Vida é composto e identificado pelos momentos vividos pela informação que a submetem ao risco. Os momentos são vivenciados justamente quando os ativos físicos, tecnológicos e humanos fazem uso da informação, sustentando processos que, por sua vez, mantêm a operação da organização. A figura a seguir apresenta uma relação entre o corpo humano e o negócio de uma empresa.

Diante das situações em que a informação é exposta a ameaças que colocam em risco suas propriedades, atingindo a sua segurança, a próxima figura revela todos os 4 momentos do ciclo de vida que são merecedores de atenção.

- **Manuseio:** Momento que a informação é criada e manipulada seja ao interagir com documentos impressos, ao transcrever informações recém-geradas em uma aplicação Web, ou no uso senha de acesso para autenticação.
- **Armazenamento** – Momento que a informação é armazenada seja em um banco de dados compartilhado, em uma anotação de documento disposta em um arquivo físico, ou, ainda em mídia digital disposta na mesa de trabalho.
- **Transporte** – Momento que a informação é transportada, seja ao encaminhar informações por correio eletrônico, ao postar um documento via aparelho de fax, ou ainda, ao falar ao telefone uma informação confidencial.
- **Descarte** – Momento que a informação é descartada, seja ao depositar na lixeira da empresa um material impresso, seja ao eliminar um arquivo eletrônico em um computador de mesa, ou ainda, ao descartar uma mídia digital usado que apresentou falha na leitura.

3 Segurança da Informação e seus Critérios

A dependência do negócio aos sistemas de informação e com o surgimento de novas tecnologias e formas de trabalho, como o comércio eletrônico, as redes virtuais privadas e os funcionários móveis, as empresas despertam para a necessidade de segurança, uma vez que se tornaram vulneráveis a um número maior de ameaças.

As redes de computadores, e consequentemente a Internet mudaram as formas como se usam sistemas de informação. As possibilidades e oportunidades de utilização são muito mais amplas que em sistemas fechados, assim como os riscos à privacidade e integridade da informação. Portanto, é muito importante que mecanismos de segurança de sistemas de informação sejam projetados de maneira a prevenir acessos não autorizados aos recursos e dados destes sistemas (Laureano, 2004).

A segurança da informação é a proteção dos sistemas de informação contra a negação de serviço a usuários autorizados, assim como contra a intrusão, e a modificação não-autorizada de dados ou informações, armazenados, em processamento ou em trânsito, abrangendo a segurança dos recursos humanos, da documentação e do material, das áreas e instalações das comunicações e computacional, assim como as destinadas a prevenir, detectar, deter e documentar eventuais ameaças a seu desenvolvimento (NBR 17999, 2003; Dias, 2000; Wadlow, 2000; Krause e Tipton, 1999).

Segurança é a base para dar ás empresas a possibilidade e a liberdade necessária para a criação de novas oportunidades de negócio. É evidente que os negócios estão cada vez mais dependentes das tecnologias e estas precisam estar de tal forma a proporcionar confidencialidade, integridade e disponibilidade – que conforme (NBR 17999, 2003; Krause e Tipton, 1999; Albuquerque e Ribeiro, 2002), são os princípios básicos para garantir a segurança da informação – das informações:

- **Confidencialidade:** A informação somente pode ser acessada por pessoas explicitamente autorizadas;

  É a proteção de Sistemas de Informação para impedir que pessoas não autorizadas tenham acesso ao mesmo. O aspecto mais importante deste item é garantir a identificação e autenticação das partes envolvidas.

- **Disponibilidade:** A informação ou sistema de computador deve estar disponível no momento em que a mesma for necessária;

- **Integridade:** A informação deve ser retornada em sua forma original no momento em que foi armazenada; É a proteção dos dados ou informações contra modificações intencionais ou acidentais não-autorizadas.

A combinação em proporções apropriadas dos itens confidencialidade, disponibilidade e integridade facilitam o suporte para que as empresas alcancem os seus objetivos, pois seus sistemas de informação serão mais confiáveis.

O item integridade não pode ser confundido com confiabilidade do conteúdo (seu significado) da informação. Uma informação pode ser imprecisa, mas deve permanecer integra (não sofrer alterações por pessoas não autorizadas).

A segurança visa também aumentar a produtividade dos usuários através de um ambiente mais organizado, proporcionando maior controle sobre os recursos de informática, viabilizando até o uso de aplicações de missão crítica.

Existem ainda, grupos de pesquisadores e autores que defendem que para uma informação ser considera segura, o sistema que o administra ainda deve respeitar:

- **Autenticidade** – Garante que a informação ou o usuário da mesma é autêntico; Atesta com exatidão, a origem do dado ou informação;
- **Não repúdio** – Não é possível negar (no sentido de dizer que não foi feito) uma operação ou serviço que modificou ou criou uma informação; Não é possível negar o envio ou recepção de uma informação ou dado;
- **Legalidade** – Garante a legalidade (jurídica) da informação; Aderência de um sistema à legislação; Característica das informações que possuem valor legal dentro de um processo de comunicação, onde todos os ativos estão de acordo com as cláusulas contratuais pactuadas ou a legislação política institucional, nacional ou internacional vigentes.
- **Privacidade** – Foge do aspecto de confidencialidade, pois uma informação pode ser considerada confidencial, mas não privada. Uma informação privada deve ser *vista / lida / alterada* somente pelo seu dono. Garante ainda, que a informação não será disponibilizada para outras pessoas (neste é caso é atribuído o caráter de confidencialidade a informação); É a capacidade de um usuário realizar ações em um sistema sem que seja identificado.

- **Auditoria** – Rastreabilidade dos diversos passos que um negócio ou processo realizou ou que uma informação foi submetida, identificando os participantes, os locais e horários de cada etapa. Auditoria em software significa uma parte da aplicação, ou conjunto de funções do sistema, que viabiliza uma auditoria; Consiste no exame do histórico dos eventos dentro de um sistema para determinar quando e onde ocorreu uma violação de segurança.

Em (Stoneburner, 2001) é sugerido que a segurança somente é obtida através da

3.1 Ameaças

Ameaça ou *threat* (em inglês). Para Shirey (2000), têm-se vários tipos de *threat*:

- **Ameaça**: Potencial violação de segurança. Existe quando houver uma circunstância, potencialidade, ação ou evento que poderia romper a segurança e causar o dano;
  - **Ameaça Inteligente**: Circunstância na qual um oponente tem a potencialidade técnica e operacional para detectar e explorar uma vulnerabilidade de um sistema;
  - **Ameaça de Análise**: Uma análise da probabilidade das ocorrências e das consequências de ações prejudiciais a um sistema;
- **Consequências de uma ameaça**: Uma violação de segurança resultado da ação de uma ameaça. Inclui: divulgação, usurpação, decepção e rompimento.

A ameaça pode ser definida como qualquer ação, acontecimento ou entidade que possa agir sobre um ativo, processo ou pessoa, através de uma vulnerabilidade e consequentemente gerando um determinado impacto. As ameaças apenas existem se houverem vulnerabilidades, sozinhas pouco fazem.

Conforme descrito em (Sêmola, 2003), as ameaças podem ser classificadas quanto a sua intencionalidade e ser divididas em grupos:

- **Naturais** – Ameaças decorrentes de fenômenos da natureza, como incêndios naturais, enchentes, terremotos, tempestades, poluição, entre outros.
- **Involuntárias** – Ameaças inconscientes, quase sempre causadas pelo desconhecimento. Oriunda de acidentes, erros, falta de energia, entre outros.
- **Voluntárias** – Ameaças propositais causadas por agentes humanos como *hackers*, invasores, espiões, ladrões, criadores e disseminadores de vírus de computador, incendiários.

Algumas outras ameaças aos sistemas de informação, as quais podem ser originadas de fatores técnicos, organizacionais e ambientais, agravados por más decisões administrativas (Laudon e Laudon, 2004).

- Ações pessoais
- Invasão pelo terminal de acesso
- Roubo de dados, serviços, equipamentos
- Incêndio
- Problemas elétricos
- Erros de usuários
- Mudanças no programa
- Problemas de telecomunicação

3.2 Ataques

Em inglês, é utilizado o termo “*attack*” para definir ataque. E existem vários tipos de ataques.

Ataque pode ser definido como um assalto ao sistema de segurança que deriva de uma ameaça inteligente, isto é, um ato inteligente que seja uma tentativa deliberada (especial no sentido de um método ou técnica) para invadir serviços de segurança e violar as políticas do sistema (Shirey, 2000).

O ataque é ato de tentar desviar dos controles de segurança de um sistema de forma a quebrar os princípios citados anteriormente.

Um ataque pode ser (Wadlow, 2000):

Ativo: tendo por resultado a alteração dos dados;

Passivo: tendo por resultado a liberação dos dados; ou

Destrutivo: visando à negação do acesso aos dados ou serviços.

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 atividade e da eficácia de contramedidas existentes.

Para implementar mecanismos de segurança deve-se classificar as formas de ataques em sistemas: Interceptação, Interrupção, Modificação e Personificação.

Interceptação: Considera-se interceptação o acesso a informações por entidades não autorizadas (violação da privacidade e confidencialidade das informações).

Interrupção: Pode ser definida como a interrupção do fluxo normal das mensagens ao destino.

Modificação: Consiste na modificação de mensagens por entidades não autorizadas, violação da integridade da mensagem.

Personificação: Considera-se personificação a entidade que acessa as informações ou transmite mensagem se passando por uma entidade autêntica, violação da autenticidade.

3.3 Vulnerabilidades

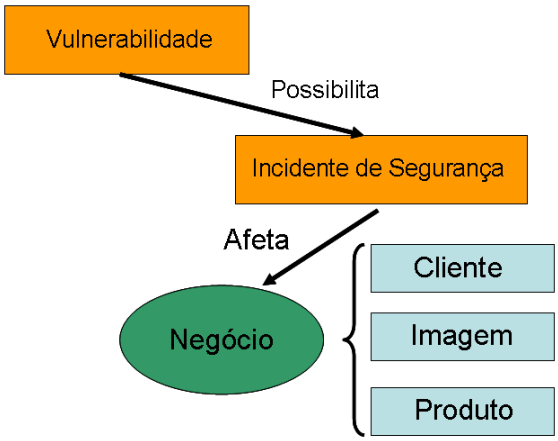
A vulnerabilidade é o ponto onde qualquer sistema é suscetível a um ataque, ou seja, é uma condição encontrada em determinados recursos, processos, configurações, entre outros que “permite” um ataque.

Todos os ambientes são vulneráveis, partindo do princípio de que não existem ambientes totalmente seguros. Por vezes são encontrados vulnerabilidades nas medidas implementadas pela empresa.

Identificar as vulnerabilidades que podem contribuir para as ocorrências de incidentes de segurança é um aspecto importante na identificação de medidas adequadas de segurança.

As vulnerabilidades estão presentes no dia-a-dia das empresas e se apresentam nas mais diversas áreas de uma organização. Não existe uma única causa para surgimento de vulnerabilidades.

Cada vulnerabilidade existente pode permitir a ocorrência de determinados incidentes de segurança. Desta forma, pode-se concluir que são as vulnerabilidades as principais causas das ocorrências de incidentes de segurança, ilustração a seguir.



3.4 Por que sistemas são vulneráveis?

Quando grande volume de dados é armazenado sob formato eletrônico, ficam vulneráveis a muito mais tipos de ameaças do que quando estão em formato manual.

Os avanços nas telecomunicações e nos sistemas de informação ampliaram essas vulnerabilidades. Sistemas de informação em diferentes localidades podem ser interconectados por meio de redes de telecomunicações. Logo, o potencial para acesso não autorizado, abuso ou fraude não fica limitado a um único lugar, mas pode ocorrer em qualquer ponto de acesso à rede.

Além disso, arranjos mais complexos e diversos de hardware, software, pessoais e organizacionais são exigidos para redes de telecomunicação, criando novas áreas e oportunidades para invasão e manipulação.

Redes sem fio que utilizam tecnologias baseadas em rádio são ainda mais vulneráveis à invasão, porque é fácil fazer a varredura das faixas de radiofrequência. A Internet apresenta problemas especiais porque foi projetada para ser acessada facilmente por pessoas com sistemas de informações diferentes. As vulnerabilidades das redes de telecomunicação estão ilustradas na próxima figura.

Redes de telecomunicação são altamente vulneráveis a falhas naturais de hardware e software e ao uso indevido por programadores, operadores de computador, pessoal de manutenção e usuário finais.

É possível, por exemplo, grampear linhas de telecomunicação e interceptar dados ilegalmente. A transmissão de alta velocidade por canais de comunicação de par trançado, por sua vez, causa à interferência denominada linha cruzada. Ou ainda, a radiação que pode causar falha da rede em vários pontos.

4 Mecanismos para Controles de Segurança

De acordo com a ISO/IEC 27002 (2005)

"*A segurança da informação é obtida a partir da implementação de um conjunto de controles adequados, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de software e hardware.*

Estes controles precisam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados, onde necessário, para garantir que os objetivos do negócio e de segurança da organização sejam atendidos.

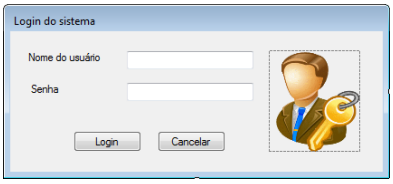
Convém que isto seja feito em conjunto com outros processos de gestão do negócio".

4.1 Autenticação e Autorização

A **autorização** é o processo de conceder ou negar direitos a usuários ou sistemas, por meio das chamadas listas de controle de acessos (*Access Control Lists* – ACL), definindo quais atividades poderão ser realizadas, desta forma gerando os chamados perfis de acesso.

A **autenticação** é o meio para obter a certeza de que o usuário ou o objeto remoto é realmente quem está afirmando ser.

Os processos de autenticação estão baseados em três métodos distintos:



Identificação positiva (O que você sabe) – É aquela na qual o requerente demonstra conhecimento de alguma informação utilizada no processo de autenticação, por exemplo, **uma senha**.

Identificação proprietária (O que você tem) – É aquela na qual o requerente demonstrar possuir algo a ser utilizado no processo de autenticação, como um **cartão magnético, dispositivo externo**.

Identificação Biométrica (O que você é) – É aquela na qual o requerente exibe alguma característica própria, tal como a sua **impressão digital, palma da mão**.

Então a autenticação:

- É um serviço essencial de segurança, pois uma autenticação confiável assegura o controle de acesso;
- Determina quem está autorizado a ter acesso à informação; e,
- Permite trilhas de auditoria (rastreabilidade) e assegura a legitimidade do acesso.

Uma autenticação forte é aquela que utiliza dispositivos externos.

Os métodos comuns de autenticação são:

Autenticação baseada em senha

- A autenticação é obtida pela verificação de um segredo;
- Mais perguntas pode aumentar o nível de autenticação;
- A autenticação por senha só prova o conhecimento, e é considerada fraca.

Fraquezas das senhas

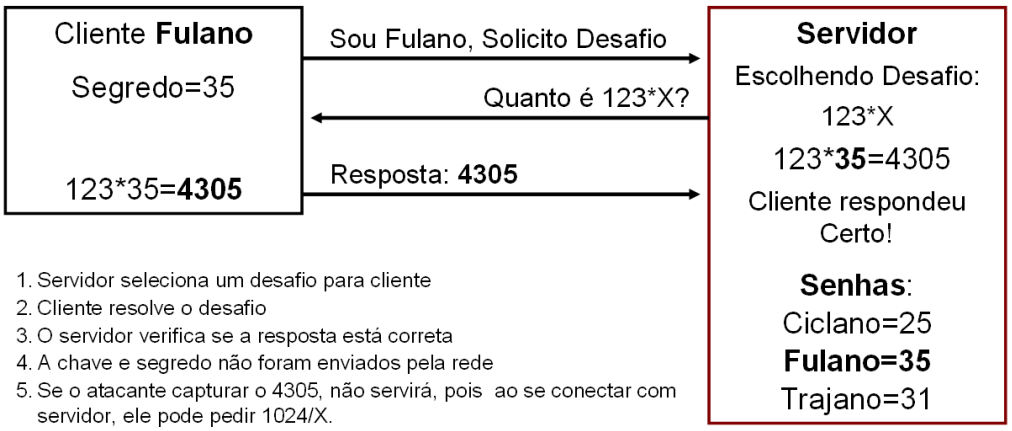
- Pessoas podem escolher senhas fracas, fáceis de adivinhar;
- Quando escolhem (ou são obrigadas a usar) senhas fortes, escrevem em um papel de fácil acesso;
- As senhas podem ser compartilhadas de forma indevida;
- Podem ser interceptadas, quando enviadas de forma desprotegida;
- Uma senha pode ser descoberta sem que o proprietário saiba.

Desafio-resposta

- Ao invés de perguntar qual é o segredo, pergunta-se sobre o segredo.
- A resposta demonstra conhecimento, sem expor o segredo.

Ex:

- Suponha que o cliente possua um segredo que é um número inteiro.
- O servidor conhece este segredo e permitirá *login* para qualquer um que provar conhecê-lo.



1. Servidor seleciona um desafio para cliente
2. Cliente resolve o desafio
3. O servidor verifica se a resposta está correta
4. A chave e segredo não foram enviados pela rede
5. Se o atacante capturar o 4305, não servirá, pois ao se conectar com servidor, ele pode pedir 1024/X.

4.2 Combate a Ataques e Invasões

Destinados a suprir a infraestrutura tecnológica com dispositivos de software e hardware de proteção, controle de acesso e consequentemente combate a ataques e invasões, esta família de mecanismos tem papel importante no modelo de gestão de segurança, à medida que as conexões eletrônicas e tentativas de acesso indevido crescem exponencialmente.

Nesta categoria, existem dispositivos destinados ao monitoramento, filtragem e registro de acessos lógicos, bem como dispositivos voltados pra a segmentação de perímetros, identificação e tratamento de tentativas de ataque.

4.2.1 Firewall

Um firewall é um sistema ou grupo de sistemas que reforçam a norma de segurança entre uma rede interna segura e uma rede não-confiável como a Internet.

Os firewalls tendem a serem vistos como uma proteção entre a Internet e a rede privada. Assim, um firewall deveria ser considerado como um meio de dividir o mundo em duas ou mais redes: uma ou mais redes seguras e uma ou mais redes não-seguras.

Um firewall pode ser um PC, um roteador, um computador de tamanho intermediário, um mainframe, uma estação de trabalho UNIX ou a combinação destes que determine qual informação ou serviços podem ser acessados de fora e a quem é permitido usar a informação e os serviços de fora.

Geralmente, um firewall é instalado no ponto onde a rede interna segura e a rede externa não-confiável se encontra ponto que também é conhecido como o ponto de estrangulamento.

Um firewall é projetado para proteger as fontes de informação de uma organização, controla o acesso entre rede interna segura e rede externa não-confiável.

É importante notar que mesmo se o firewall tiver sido projetado para:

- Permitir que dados confiáveis passem;
- Negar serviços vulneráveis e
- Proteger a rede interna contra ataques externos.

Um ataque recém-criado pode penetrar o firewall a qualquer hora. O administrador da rede examina regularmente os registros de eventos e alarmes gerados pelo firewall.

As classes de firewalls: Filtros de Pacote, Servidores Proxy e Inspeção de Estado.

4.2.1.1 Filtros de Pacotes

A filtragem de pacotes é um dos principais mecanismos que, mediante regras definidas pelo administrador em um firewall, permite ou não a passagem de Datagramas IP em uma rede.

O Pacote possui um cabeçalho com diversas informações a seu respeito, como endereço IP de origem, endereço IP do destino, tipo de serviço, tamanho, entre outros.

O Firewall analisa estas informações de acordo com as regras estabelecidas para liberar ou não o pacote (seja para sair ou para entrar na máquina/rede), podendo também executar alguma tarefa relacionada, como registrar o acesso (ou tentativa de) em um arquivo de log. Deste modo, é possível filtrar pacotes para impedir o acesso a um serviço de Telnet, um chat ou mesmo um site na Internet.

A transmissão dos dados é feita com base no padrão TCP/IP, que é organizado em camadas. A filtragem normalmente se limita às Camadas de Rede e de Transporte.

- **Camada de Rede**: é onde ocorre o endereçamento dos equipamentos que fazem parte da rede e processos de roteamento, por exemplo;
- **Camada de Transporte**: é onde estão os protocolos que permitem o tráfego de dados, como o TCP e o UDP.

O processo de filtragem de pacotes pode ser: Filtros Estáticos e Filtros Dinâmicos.

a) Filtros Estáticos

Os dados são bloqueados ou liberados com base nas regras, não importando a ligação que cada pacote tem com outro.

Esta abordagem não é um problema, mas determinados serviços ou aplicativos podem depender de respostas ou requisições específicas para iniciar e manter a transmissão. Ou seja, é possível filtros com regras que permitem o tráfego destes serviços, mas ao mesmo tempo bloqueiem respostas e/ou requisições necessárias, impedindo a execução da tarefa.

Neste caso, ocasionar o enfraquecimento da segurança, uma vez que um administrador poderia criar regras menos rígidas para evitar que os serviços sejam impedidos de trabalhar, aumentando os riscos de o firewall não filtrando pacotes que deveriam ser, de fato, bloqueados

b) Filtros Dinâmicos

Nesta categoria, os filtros consideram o contexto em que os pacotes estão inseridos para “criar” regras que se adaptam ao cenário, permitindo que determinados pacotes trafeguem, mas somente quando necessário e durante o período correspondente. Desta forma, as chances de respostas de serviços serem barradas, por exemplo, cai consideravelmente.

4.2.2 Firewalls Pessoais

Existe firewall simples destinados a proteger o computador pessoal, seja ele um desktop, um laptop, um tablet, enfim, são os **firewalls pessoais** ou domésticos, que podem ser utilizados por qualquer pessoa.

Os Sistemas Operacionais. para uso doméstico ou em escritório costumam conter firewall interno por padrão, como é o caso de distribuições Linux, do Windows 8, 10 ou do Mac OS X. Ainda, é comum desenvolvedores de antivírus oferecerem opções de proteção junto ao software, entre elas, um firewall.

Solução mais eficiente e que permita vários tipos de ajustes é possível encontrar, muitas delas gratuitas.

Por exemplo: Usuários de Windows, podem contar com o ZoneAlarm, com o Comodo, entre outros.

4.2.3 Detector de Intrusos

A maneira mais comum para descobrir intrusões é a utilização dos dados das auditorias gerados pelos sistemas operacionais e ordenados em ordem cronológica de acontecimento, sendo possível à inspeção manual destes registros, o que não é uma prática viável, pois estes arquivos de *logs* apresentam tamanhos consideráveis.

Nos últimos anos, a tecnologia de detecção de intrusão, IDS - Intrusion Detection System tem se mostrado uma grande aliada dos administradores de segurança.

Basicamente, o que tais sistemas fazem é tentar reconhecer um comportamento ou uma ação intrusiva, através da análise das informações disponíveis em um sistema de computação ou rede, para alertar um administrador e/ou automaticamente disparar contramedidas.

Para realizar a detecção, várias tecnologias estão sendo empregadas em produtos comerciais ou em projetos de pesquisas, as tecnologias utilizadas incluem:

Análise Estatística, Inferência, IA, Data Mining, Redes Neurais e diversas outras.

Um IDS automatiza a tarefa de analisar dados da auditoria. Estes dados são extremamente úteis, pois podem ser usados para estabelecer a culpabilidade do atacante e na maioria das vezes é o único modo de descobrir uma atividade sem autorização, detectar a extensão dos danos e prevenir tal ataque no futuro.

Desta forma o IDS torna-se uma ferramenta extremamente valiosa para análises em tempo real e também após a ocorrência de um ataque.

4.2.4 Classificação de Detectores de Intrusão

O IDS tem como principal objetivo detectar se alguém está tentando entrar em um sistema ou se algum usuário legítimo está fazendo inadequado uso do mesmo. Esta ferramenta é executada constantemente em *background* e somente gera uma notificação quando detecta alguma ocorrência que seja suspeita ou ilegal.

Os sistemas em uso podem ser classificados com relação a sua forma de monitoração (origem dos dados) e aos mecanismos (algoritmos) utilizados de detecção.

4.2.4.1 Quanto à Origem dos Dados

Existem basicamente dois tipos de implementação de ferramentas IDS.

Os sistemas NIDS, Network Based IDS, podem monitorar diversos computadores simultaneamente. Todavia, sua eficácia diminui na medida em que o tamanho e a velocidade da rede aumenta, pela necessidade de analisar os pacotes mais rapidamente. Além disso, o uso de protocolos cifrados (baseados em SSL – Secure Socket Layer) torna o conteúdo dos pacotes opaco ao IDS.

A velocidade da rede e o uso de criptografia não são problemas para os sistemas HIDS, Host Based IDS. Todavia, como esse sistema é instalado na própria máquina a monitorar, pode ser desativado por um invasor bem-sucedido.

Existem IDS que trabalham de forma híbrida, combinando as duas técnicas citadas anteriormente.

4.2.4.2 Quanto à Forma de Detecção

Muitas ferramentas de IDS realizam suas operações a partir da análise de padrões do sistema operacional e da rede tais como:

- Utilização de CPU, E/S de disco,
- Uso de memória,
- Atividades dos usuários,
- Número de tentativas de *login*,
- Número de conexões,
- Volume de dados trafegando no segmento de rede entre outros.

Estes dados formam uma base de informação sobre a utilização do sistema em vários momentos ao longo do dia.

Algumas ferramentas possuem bases com padrões de ataque (assinaturas) previamente constituído, permitindo também a configuração das informações já existentes bem como inclusão de novos parâmetros. As técnicas usadas para detectar intrusões podem ser classificadas em:

- **Detecção por Assinatura** – os dados coletados são comparados com uma base de registros de ataques conhecidos (assinaturas). Por exemplo, o sistema pode vasculhar os pacotes de rede procurando sequências de bytes que caracterizem um ataque de *buffer overflow* contra o servidor Apache;
- **Detecção por Anomalia** – os dados coletados são comparados com registros históricos da atividade considerada normal do sistema. Desvios da normalidade são sinalizados como ameaças.
- **Detecção Híbrida** – o mecanismo de análise combina as duas abordagens anteriores, buscando detectar ataques conhecidos e comportamentos anormais.

A detecção por assinatura é a técnica mais empregada nos sistemas de produção atuais. Um exemplo de IDS baseado em assinatura é o SNORT. Os sistemas antivírus também adotam a detecção por assinatura. A detecção de intrusão por anomalia ainda é pouco usada em sistemas de produção.

4.3 Privacidade das Comunicações

Por privacidade entende-se o direito de cada indivíduo ou organização de manter e controlar o conjunto de informações que o cerca, podendo decidir-se, quando, por que e por quem essas informações podem ser obtidas e usadas. Privacidade envolve ainda o direito de permanecer livre de intrusos e autônomo.

Para garantir o conceito de privacidade no contexto das comunicações alguns instrumentos e metodologias são apresentados a seguir.

4.3.1 Criptografia

A palavra criptografia tem origem grega (*kriptos* = escondido, oculto e grifo = grafia, escrita) e define a arte ou ciência de escrever em cifras ou em códigos, utilizando um conjunto de técnicas que torna uma mensagem incompreensível, chamada comumente de texto cifrado, através de um processo chamado cifragem, permitindo que apenas o

destinatário desejado consiga decodificar e ler a mensagem com clareza, no processo inverso, a decifragem.

Criptografia é a ciência de escrever ocultamente e hoje, sem dúvida, é a maneira mais segura de se enviar informações através de um canal de comunicação inseguro como, por exemplo, a Internet.

A criptografia representa um conjunto de técnicas que são usadas para manter a informação segura. Estas técnicas consistem na utilização de chaves e algoritmos de criptografia. Tendo conhecimento da chave e do algoritmo usado é possível desembaralhar a mensagem recebida.

Existem dois tipos de criptografia, cada uma com características, vantagens e desvantagens: Criptografia Simétrica e Criptografia Assimétrica.

- A **Criptografia Simétrica**: basicamente é usada apenas uma chave para cifrar e decifrar o texto.
- A **Criptografia Assimétrica**: usa uma chave para cifrar e uma outra para decifrar a mensagem.

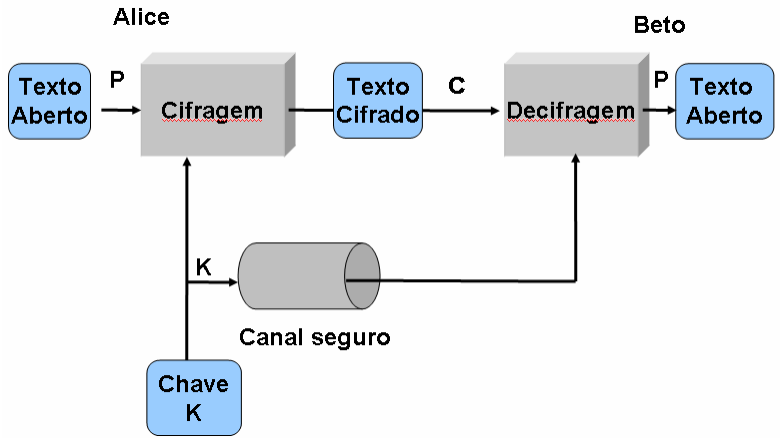
4.3.1.1 Criptografia Simétrica ou de Chave Privada

São os algoritmos convencionais de criptografia e a mesma chave secreta tanto é utilizada para cifrar como para decifrar uma mensagem, devendo ser conhecida por ambos os lados do processo.

Este é o grande problema do método, pois a chave tem de ser entregue aos participantes de modo seguro, e as transações só podem ser realizadas depois disso.

O fato de ambos os lados conhecerem a chave também leva à possibilidade de repúdio da transação, pois um lado pode sempre alegar que o outro usou a chave e realizou a transação em seu nome, indevidamente.

Como cada par de participantes deve ter uma chave própria, o número de chaves necessárias para comunicação segura entre muitos participantes cresce, com agravante adicional de que todas essas chaves são secretas e devem ser protegidas adequadamente. Ou seja, um participante do ciclo de criptografia deverá ter a chave de todos os outros para se comunicar com cada um deles. Isso inviabiliza o uso destes algoritmos isoladamente em certas aplicações.



Os algoritmos de chave simétrica são usados para cifrar a maioria dos dados ou fluxos de dados. Estes algoritmos são projetados para serem bem rápidos e (geralmente) terem um grande número de chaves possíveis.

Os melhores algoritmos de chave simétrica oferecem boa segurança quando os dados são cifrados com determinada chave, e dificilmente pode-se decifrar os dados sem possuir a mesma chave.

Como a criptografia é sempre uma carga adicional ao processamento, esta vantagem é importante e deverá ser utilizada adequadamente.

Há muitos algoritmos de chave simétrica em uso atualmente. Alguns dos algoritmos mais comuns no campo da segurança são:

- **DES**
- **Triple DES**
- **IDEA**
- **RC2**
- **RC4**
- **RC5**
- **RC6**
- **Blowfish**
- **Twofish**

4.3.1.2 Criptografia Assimétrica ou de Chave Pública

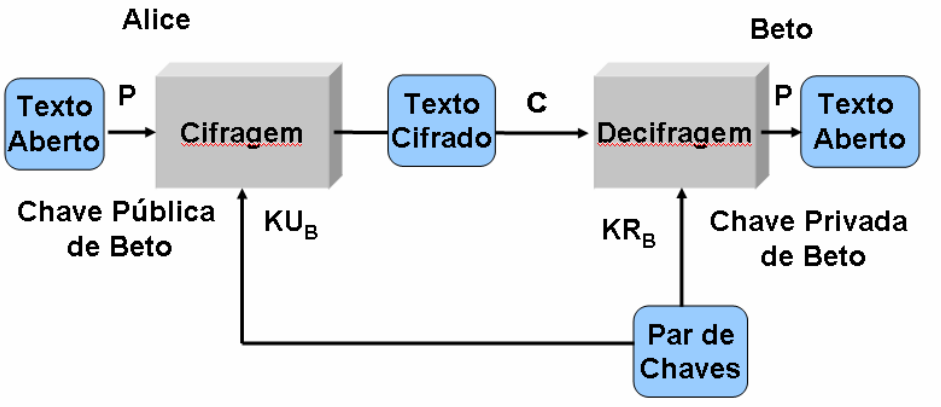
A existência da criptografia de chave pública foi postulada pela primeira vez em meados de 1975 por Withfield Diffie e Martin Hellman.

Os pesquisadores, na época na universidade de Stanford, escreveram um artigo em que pressuponham a existência de uma técnica criptográfica com a qual a informação criptografada com uma chave poderia ser decifrada por uma segunda chave, aparentemente sem relação com a primeira.

Robert Merkle, então estudante em Berkeley que tinha ideias semelhantes mas, devido à lentidão do processo de publicação acadêmica, seus artigos só foram publicados quando a ideia de criptografia de chave pública já era bem conhecida.

Os algoritmos assimétricos utilizam duas chaves diferentes, uma em cada extremidade do processo. As duas chaves são associadas através de um relacionamento matemático, pertencendo a apenas um participante, que as utilizará para se comunicar com todos os outros de modo seguro.

Essas duas chaves são geradas de tal maneira que a partir de uma delas não é possível calcular a outra a um custo computacional viável, possibilitando a divulgação de uma delas, denominada chave pública, sem colocar em risco o segredo da outra, denominada chave secreta ou privada.



Os principais sistemas de chaves públicas atualmente em uso são:

- **Diffie-Hellman**
- **ElGamal**
- **DSS**
- **RSA**

4.3.2 Comparação entre Métodos de Criptografia

Afinal diante das inúmeras vantagens da criptografia assimétrica, então em que contexto deve-se considerar a criptografia simétrica.

Como quantificar as dificuldades de se gerar as chaves de maneira segura e os problemas relativos à performance.

	Criptografia Simétrica	**Criptografia Assimétrica**
Funcionamento	O mesmo algoritmo é usado para criptografar e descriptografar a mensagem.	O mesmo algoritmo é usado para criptografar e descriptografar a mensagem, porém usando duas chaves
Requer	Que o destino e origem saibam o algoritmo e a chave.	A origem e o destino devem saber uma (somente uma) chave do par de chaves. Todos podem ter a chave pública, porém só 1 deve saber a chave privada
Segurança	A chave deve ser mantida em segredo. Mesmo sabendo o algoritmo e tendo exemplos dos textos criptografados deve impossibilitar a determinação da chave.	Apenas 1 das duas chaves deve ser mantida em segredo É impossível decifrar uma mensagem mesmo tendo acesso ao algoritmo, à chave pública e a exemplos dos textos cifrados. Tendo a chave pública deve ser impossível chegar na chave privada.
Utilidade	Privacidade	Identificação; Assinatura Digital; Privacidade; Troca de Chaves e muitas outras utilidades.
Velocidade de Processamento	Muito Rápida	Lenta
Segurança	Alta	Alta
Chaves	Uma	Duas Chaves (Pública e Privada)

4.3.3 Assinatura Digital

Outra grande vantagem dos algoritmos assimétricos, particularmente o RSA, que é o mais conhecido e utilizado atualmente, é que o processo funciona também na criptografia no outro sentido, da chave secreta para a chave pública, o que possibilita implementar o que se denomina assinatura digital.

O conceito de assinatura é o de um processo que apenas o signatário possa realizar, garantindo dessa maneira sua participação pessoal no processo. Como a chave secreta é de posse e uso exclusivo de seu detentor, um processo de cifragem usando a chave privada do signatário se encaixa nesse conceito, permitindo, assim, a geração de uma assinatura por um processo digital.

- **No caso da assinatura digital**, é inadequado cifrar toda a mensagem ou documento a ser assinado digitalmente devido ao tempo gasto na criptografia de um documento utilizando chaves assimétricas. A criptografia é aplicada apenas sobre um identificador unívoco do mesmo.
- **No caso da criptografia** é normalmente é utilizado como identificador o resultado da aplicação de uma função tipo HASH, que mapeia um documento digital de tamanho qualquer num conjunto de bits de tamanho fixo.

Ao valor do HASH pode ainda ser anexada a data/hora, número de sequência e outros dados identificadores, e este conjunto é então cifrado com a chave secreta do signatário constituindo a assinatura digital do documento.

A função de HASH será explicada em um fluxograma a seguir.

Qualquer participante pode verificar a autenticidade de uma assinatura digital, bastando decifrá-la com a chave pública do signatário, o qual todos podem ter acesso. Se o resultado é significativo, está garantido o uso da chave secreta correspondente na assinatura e, portanto sua autenticidade.

Resta ainda comprovar a associação da assinatura ao documento, o que é feito recalculando o HASH do documento recebido e comparando-o com o valor incluído na assinatura. Sendo iguais, prova-se ainda a ligação com o documento, assim como a integridade (não alteração) do mesmo. Como a verificação é realizada utilizando a chave pública, sua validação pode ser realizada por terceiros, tais como árbitros e auditores.

4.3.4 Infraestrutura de Chaves Públicas

Uma **Infraestrutura de Chaves Públicas**, cujo sigla é **ICP**, é um órgão ou iniciativa pública ou privada que tem como objetivo manter uma estrutura de emissão de chaves públicas, baseando-se no princípio da terceira parte confiável, oferecendo uma mediação de credibilidade e confiança em transações entre partes que utilizam certificados digitais.

A principal função do ICP é definir um conjunto de técnicas, práticas e procedimentos a serem adotados pelas entidades a fim de estabelecer um sistema de certificação digital baseado em chave pública. A infra-estrutura de chaves públicas do Brasil, definida pela Medida Provisória Nº 2.200-2, de 24 de Agosto de 2001, é denominada Infraestrutura de Chaves Públicas Brasileira, ou ICP-Brasil.

4.3.4.1 ICP-Brasil

A Infraestrutura de Chaves Públicas Brasileira ou ICP-Brasil é um conjunto de entidades governamentais ou de iniciativa privada, padrões técnicos e regulamentos, elaborados para suportar um sistema criptográfico com base em certificados digitais e visa assegurar as transações entre titulares de certificados digitais e detentores de chaves públicas.

Para assegurar que uma determinada chave pertence a “você” é necessário que uma Autoridade Certificadora (AC) confira sua identidade e seus respectivos dados. Ela será a entidade responsável pela emissão, suspensão, renovação ou revogação de seu certificado digital, além de ser obrigada a manter sempre disponível a Lista de Certificados Revogados (CRL).

A ICP–Brasil é formada por uma Autoridade Certificadora Raiz (AC-RAIZ) que é representada pelo Instituto Nacional de Tecnologia da Informação (ITI), sendo este órgão responsável pela autentificação das demais Autoridades Certificadoras, além de executar atividades de fiscalização e auditoria das AC e Autoridades de Registro (AR) para que possa certificar-se de que a entidade está seguindo todas as Políticas de Certificação.

A Certificação Digital permite que informações transitem pela Internet com maior segurança. Utilizando-se da Certificação Digital, é possível, por exemplo, evitar que crackers interceptem ou adulterem as comunicações realizadas via Internet. Também é possível saber, com certeza, quem foi o autor de uma transação ou de uma mensagem, ou, ainda, manter dados confidenciais protegidos contra a leitura por pessoas não autorizadas.

Principais vantagens:

- **Garantia de sigilo e privacidade** – Quando se visita um site "seguro" da web, o seu computador recebe o certificado contendo a chave pública desse site, o que é suficiente para criar um túnel criptográfico, tornando os dados incompreensíveis durante o tráfego, sendo possível apenas ao servidor web recuperar a informação original.

- **Controle de acesso a aplicativos** – O servidor web pode solicitar ao usuário que apresente um certificado digital, em vez de digitar usuário e senha. Os usuários não poderão colocar em perigo a aplicação pela falta de cuidado no uso e armazenamento da senha.
- **Assinatura de formulários e impossibilidade de repúdio** – Os usuários poderão assinar os formulários que submetem preenchidos pela web da mesma maneira que fariam pessoalmente em um balcão de atendimento.
- **Garantia de sigilo e privacidade** – O sistema de correio eletrônico utilizado para troca de mensagens através da Internet não possui recursos nativos para impedir a violação da correspondência eletrônica.

  Com o uso de certificados digitais, pode-se selar a sua correspondência em um envelope digital criptográfico e certificar-se de que apenas o destinatário será capaz de compreender seu conteúdo.
- **Identificação do remetente** – Não existirá mais dúvidas sobre a origem de uma mensagem, pois será possível certificar-se da identidade do emissor.
- **Assinatura de mensagens e impossibilidade de repúdio** – As mensagens de correio eletrônico, ou qualquer documento digital passam a valer como documento assinado, com validade jurídica, dispensando-se o uso de papel.

4.3.4.2 Filiação a ICP-Brasil

Qualquer pessoa física ou jurídica pode obter uma certificação, através de uma Autoridade de Registro (AR), portando documentos necessários.

Deve ser efetuada a identificação pessoal do futuro titular do certificado, uma vez que este documento eletrônico será a sua "carteira de identidade" no mundo virtual. Assim, para a emissão do certificado tanto o interessado pode ir à AR como a AR pode ir ao cliente identificá-lo.

Um arquivo com a estrutura detalhada da ICP-Brasil, assim como a estrutura resumida - contendo apenas as Autoridades Certificadoras de 1º Nível e de 2º Nível - é fornecido pelo ITI em Estrutura da ICP-Brasil.