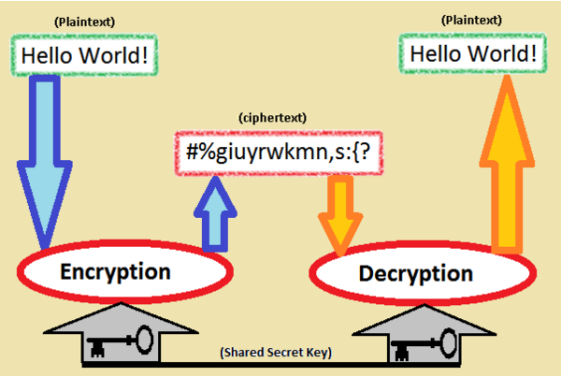
Segurança da informação



A criptografia é essencial para a troca de dados pela internet.

A **segurança da informação** está diretamente relacionada com proteção de um conjunto de informações, no sentido de preservar o valor que possuem para um indivíduo ou uma organização. São características básicas da segurança da informação os atributos de confidencialidade, integridade, disponibilidade e autenticidade, não estando esta segurança restrita somente a sistemas computacionais, informações eletrônicas ou sistemas de armazenamento. O conceito se aplica a todos os aspectos de proteção de informações e dados. O conceito de *Segurança Informática* ou *Segurança de Computadores* está intimamente relacionado com o de Segurança da Informação, incluindo não apenas a segurança dos dados/informação, mas também a dos sistemas em si.

Atualmente o conceito de Segurança da Informação está padronizado pela norma ISO/IEC 17799:2005, influenciada pelo padrão inglês (British Standard) BS 7799. A série de normas ISO/IEC 27000 foram reservadas para tratar de padrões de Segurança da Informação, incluindo a complementação ao trabalho original do padrão inglês. A ISO/IEC 27002:2005 continua sendo considerada formalmente como 17799:2005 para fins históricos. A partir de 2013 a norma técnica de segurança da informação em vigor é: ABNT NBR ISO/IEC 27002:2013 [1]

1 Conceitos de segurança

A maioria das definições de Segurança da Informação (SI) (Brostoff, 2004; Morris e Thompson, 1979; Sieberg, 2005; Smith, 2002;) pode ser sumarizada como a proteção contra o uso ou acesso não-autorizado à informação, bem como a proteção contra a negação do serviço a usuários autorizados, enquanto a integridade e a confidencialidade dessa informação são preservadas. A SI não está confinada a sistemas de computação, nem à informação em formato eletrônico. Ela se aplica a todos os aspectos de proteção da informação ou dados, em qualquer forma. O nível de proteção deve, em qualquer situação, corresponder ao valor dessa informação e aos prejuízos que poderiam decorrer do uso impróprio da mesma. É importante lembrar que a SI também cobre toda a infraestrutura que permite o seu uso, como processos, sistemas, serviços, tecnologias, e outros.

A Segurança da Informação se refere à proteção existente sobre as informações de uma determinada empresa ou pessoa, isto é, aplica-se tanto as informações corporativas quanto às pessoais. Entende-se por informação todo e qualquer conteúdo ou dado que tenha valor para alguma organização ou pessoa. Ela pode estar guardada para uso restrito ou exposta ao público para consulta ou aquisição.

Podem ser estabelecidas métricas (com o uso ou não de ferramentas) para a definição do nível de segurança existente e, com isto, serem estabelecidas as bases para análise da melhoria ou piora da situação de segurança existente. A segurança de uma determinada informação pode ser afetada por fatores comportamentais e de uso de quem se utiliza dela, pelo ambiente ou infraestrutura que a cerca ou por pessoas mal intencionadas que têm o objetivo de furtar, destruir ou modificar tal informação.

A tríade CIA (Confidentiality, Integrity and Availability) -- Confidencialidade, Integridade e Disponibilidade -- representa os principais atributos que, atualmente, orientam a análise, o planejamento e a implementação da segurança para um determinado grupo de informações que se deseja proteger. Outros atributos importantes são a irretratabilidade, a autenticidade e a conformidade. Com a evolução do comércio eletrônico e da sociedade da informação, a privacidade é também uma grande preocupação.

Portanto os atributos básicos, segundo os padrões internacionais (ISO/IEC 17799:2005) são os seguintes:

- *Confidencialidade* - propriedade que limita o acesso a informação tão somente às entidades legítimas, ou seja, àquelas autorizadas pelo proprietário da informação.
- *Integridade* - propriedade que garante que a informação manipulada mantenha todas as características originais estabelecidas pelo proprietário da informação, incluindo controle de mudanças e garantia do seu ciclo de vida (nascimento,manutenção e

destruição).

- *Disponibilidade* - propriedade que garante que a informação esteja sempre disponível para o uso legítimo, ou seja, por aqueles usuários autorizados pelo proprietário da informação.
- *Autenticidade* - propriedade que garante que a informação é proveniente da fonte anunciada e que não foi alvo de mutações ao longo de um processo.
- *Irretratabilidade* - propriedade que garante a impossibilidade de negar a autoria em relação a uma transação anteriormente feita
- Conformidade: propriedade que garante que o sistema deve seguir as leis e regulamentos associados a este tipo de processo.

Para a montagem desta política, deve-se levar em conta:

- Riscos associados à falta de segurança;
- Benefícios;
- Custos de implementação dos mecanismos.

2 Mecanismos de segurança

O suporte para as recomendações de segurança pode ser encontrado em:

- **Controles físicos**: são barreiras que limitam o contato ou acesso direto a informação ou a infraestrutura (que garante a existência da informação) que a suporta.

Existem mecanismos de segurança que apoiam os controles físicos:

Portas / trancas / paredes / blindagem / guardas / etc ..

- **Controles lógicos**: são barreiras que impedem ou limitam o acesso a informação, que está em ambiente controlado, geralmente eletrônico, e que, de outro modo, ficaria exposta a alteração não autorizada por elemento mal intencionado.

Existem mecanismos de segurança que apóiam os controles lógicos:

- **Mecanismos de cifração ou encriptação**: Permitem a transformação reversível da informação de forma a torná-la ininteligível a terceiros. Utiliza-se para tal, algoritmos determinados e uma chave secreta para, a partir de um conjunto de dados não criptografados, produzir uma sequência de dados criptografados. A operação inversa é a decifração.
- **Assinatura digital**: Um conjunto de dados criptografados, associados a um documento do qual são função, garantindo a integridade e autenticidade do documento associado, mas não a sua confidencialidade.
- **Mecanismos de garantia da integridade da informação**: Usando funções de "Hashing" ou de checagem, é garantida a integridade através de comparação do resultado do teste local com o divulgado pelo autor.
- **Mecanismos de controle de acesso**: Palavras-chave, sistemas biométricos, firewalls, cartões inteligentes.
- **Mecanismos de certificação**: Atesta a validade de um documento.
- **Integridade**: Medida em que um serviço/informação é genuíno, isto é, está protegido contra a personificação por intrusos.
- **Honeypot**: É uma ferramenta que tem a função de propositalmente simular falhas de segurança de um sistema e colher informações sobre o invasor enganando-o, fazendo-o pensar que esteja de fato explorando uma vulnerabilidade daquele sistema. É uma espécie de armadilha para invasores. O HoneyPot não oferece nenhum tipo de proteção.
- **Protocolos seguros**: Uso de protocolos que garantem um grau de segurança e usam alguns dos mecanismos citados aqui.

Existe hoje em dia um elevado número de ferramentas e sistemas que pretendem fornecer segurança. Alguns exemplos são os detectores de intrusões, os antivírus, firewalls, firewalls locais, filtros anti-spam, fuzzers, analisadores de código etc.[2]

3 Ameaças à segurança

As ameaças à segurança da informação são relacionadas diretamente à perda de uma de suas 3 características principais, quais sejam:

- **Perda de Confidencialidade**: seria quando há uma quebra de sigilo de uma determinada informação (ex: a senha de um usuário ou administrador de sistema) permitindo que sejam expostas informações restritas as quais seriam acessíveis apenas por um determinado grupo de usuários.
- **Perda de Integridade**: aconteceria quando uma determinada informação fica exposta a manuseio por uma pessoa não autorizada, que efetua alterações que não foram aprovadas e não estão sob o controle do proprietário (corporativo ou privado) da informação.

- **Perda de Disponibilidade**: acontece quando a informação deixa de estar acessível por quem necessita dela. Seria o caso da perda de comunicação com um sistema importante para a empresa, que aconteceu com a queda de um servidor ou de uma aplicação crítica de negócio, que apresentou uma falha devido a um erro causado por motivo interno ou externo ao equipamento ou por ação não autorizada de pessoas com ou sem má intenção.

No caso de ameaças à rede de computadores ou a um sistema, estas podem vir de agentes maliciosos, muitas vezes conhecidos como crackers, (hackers não são agentes maliciosos, pois tentam ajudar a encontrar possíveis falhas). Estas pessoas são motivadas para fazer esta ilegalidade por vários motivos. Os principais são: notoriedade, auto-estima, vingança e o dinheiro. De acordo com pesquisa elaborada pelo Computer Security Institute (), mais de 70% dos ataques partem de usuários legítimos de sistemas de informação (Insiders) -- o que motiva corporações a investir largamente em controles de segurança para seus ambientes corporativos (intranet).

4 Invasões na Internet

Todo sistema de computação necessita de um sistema para proteção de arquivos. Este sistema é um conjunto de regras que garantem que a informação não seja lida, ou modificada por quem não tem permissão. A segurança é usada especificamente para referência do problema genérico do assunto, já os mecanismos de proteção são usados para salvar as informações a serem protegidas. A segurança é analisada de várias formas, sendo os principais problemas causados com a falta dela a perda de dados e as invasões de intrusos. A perda de dados na maioria das vezes é causada por algumas razões: fatores naturais: incêndios, enchentes, terremotos, e vários outros problemas de causas naturais; Erros de hardware ou de software: falhas no processamento, erros de comunicação, ou bugs em programas; Erros humanos: entrada de dados incorreta, montagem errada de disco ou perda de um disco. Para evitar a perda destes dados é necessário manter um backup confiável, guardado longe destes dados originais.

4.1 Exemplos de Invasões

O maior acontecimento causado por uma invasão foi em 1988, quando um estudante colocou na internet um programa malicioso (worm), derrubando milhares de computadores pelo mundo, que foi identificado e removido logo após. Mas até hoje há controvérsias de que ele não foi completamente removido da rede. Esse programa era feito em linguagem C, e não se sabe até hoje qual era o objetivo, o que se sabe é que ele tentava descobrir todas as senhas que o usuário digitava. Mas esse programa se auto-copiava em todos os computadores em que o estudante invadia. Essa “brincadeira” não durou muito, pois o estudante foi descoberto pouco tempo depois, processado e condenado a liberdade condicional, e teve que pagar uma alta multa.

Um dos casos mais recentes de invasão por meio de vírus foi o do Vírus Conficker (ou Downup, Downadup e Kido) que tinha como objetivo afetar computadores dotados do sistema operacional Microsoft Windows, e que foi primeiramente detectado em outubro de 2008. Uma versão anterior do vírus propagou-se pela internet através de uma vulnerabilidade de um sistema de rede do Windows 2000, Windows XP, Windows Vista, Windows Server 2003, Windows Server 2008, Windows 7 Beta e do Windows Server 2008 R2 Beta, que tinha sido lançado anteriormente naquele mês. O vírus bloqueia o acesso a websites destinados à venda, protegidos com sistemas de segurança e, portanto, é possível a qualquer usuário de internet verificar se um computador está infectado ou não, simplesmente por meio do acesso a websites destinados a venda de produtos dotados de sistemas de segurança. Em janeiro de 2009, o número estimado de computadores infectados variou entre 9 e 15 milhões. Em 13 de fevereiro de 2009, a Microsoft estava oferecendo 250.000 dólares americanos em recompensa para qualquer informação que levasse à condenação e à prisão de pessoas por trás da criação e/ou distribuição do Conficker. Em 15 de outubro de 2008, a Microsoft liberou um patch de emergência para corrigir a vulnerabilidade MS08-067, através da qual o vírus prevalece-se para poder se espalhar. As aplicações da atualização automática se aplicam somente para o Windows XP SP2, SP3, Windows 2000 SP4 e Windows Vista; o Windows XP SP1 e versões mais antigas não são mais suportados. Os softwares antivírus não-ligados a Microsoft, tais como a BitDefender, Enigma Software, Eset,F-Secure, Symantec, Sophos, e o Kaspersky Lab liberaram atualizações com programas de detecção em seus produtos e são capazes de remover o vírus. A McAfee e o AVG também são capazes de remover o vírus através de escaneamentos de discos rígidos e mídias removíveis.

Através desses dados vemos que os antivírus devem estar cada vez mais atualizados, estão surgindo novos vírus rapidamente, e com a mesma velocidade deve ser lançado atualizações para os bancos de dados dos antivírus para que os mesmos sejam identificados e excluídos. Com a criação da internet essa propagação de vírus é muito rápida e muito perigosa, pois se não houver a atualização dos antivírus o computador e usuário estão vulneráveis, pois com a criação da internet várias empresas começarão a utilizar internet como exemplo empresas mais precisamente bancos, mas como é muito vulnerável esse sistema, pois existem vírus que tem a capacidade de ler o teclado (in/out), instruções privilegiadas como os keyloggers. Com esses vírus é possível ler a senha do usuário que acessa sua conta no banco, com isso é mais indicado utilizar um teclado virtual para digitar as senhas ou ir di-

retamente ao banco.

5 Nível de segurança

Depois de identificado o potencial de ataque, as organizações têm que decidir o nível de segurança a estabelecer para uma rede ou sistema os recursos físicos e lógicos a necessitar de proteção. No nível de segurança devem ser quantificados os custos associados aos ataques e os associados à implementação de mecanismos de proteção para minimizar a probabilidade de ocorrência de um ataque.

5.1 Segurança física

Considera as ameaças físicas como incêndios, desabamentos, relâmpagos, alagamento, algo que possa danificar a parte física da segurança, acesso indevido de estranhos, forma inadequada de tratamento e manuseio do veículo.

5.2 Segurança lógica

Atenta contra ameaças ocasionadas por vírus, acessos remotos à rede, *backup* desatualizados, violação de senhas, furtos de identidades, etc.

Segurança lógica é a forma como um sistema é protegido no nível de sistema operacional e de aplicação. Normalmente é considerada como proteção contra ataques, mas também significa proteção de sistemas contra erros não intencionais, como remoção acidental de importantes arquivos de sistema ou aplicação.

6 Pontos de Controle de Segurança

[3]Conforme Bluephoenix(2008)apud Santos(2012), após identificar os riscos, os níveis de proteção e determinar as decorrências que os riscos podem causar, deve-se executar os pontos de controle para reduzir riscos. Os controles podem aplicar-se na seguinte forma:

1. Políticas de Segurança da informação;
2. Organização da Segurança da Informação;
3. Gestão e Controle de Ativos;
4. Segurança em Recursos Humanos;
5. Segurança Física e do Ambiente;
6. Gestão das Operações e Comunicações;
7. Controle de Acessos;
8. Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação;
9. Gestão da Continuidade do Negócio;
10. Conformidade Legal.

7 Políticas de segurança

De acordo com o RFC 2196 (*The Site Security Handbook*), uma política de segurança consiste num conjunto formal de regras que devem ser seguidas pelos utilizadores dos recursos de uma organização.

As políticas de segurança devem ter implementação realista, e definir claramente as áreas de responsabilidade dos utilizadores, do pessoal de gestão de sistemas e redes e da direção. Deve também adaptar-se a alterações na organização. As políticas de segurança fornecem um enquadramento para a implementação de mecanismos de segurança, definem procedimentos de segurança adequados, processos de auditoria à segurança e estabelecem uma base para procedimentos legais na sequência de ataques.

O documento que define a política de segurança deve deixar de fora todos os aspectos técnicos de implementação dos mecanismos de segurança, pois essa implementação pode variar ao longo do tempo. Deve ser também um documento de fácil leitura e compreensão, além de resumido.

Algumas normas definem aspectos que devem ser levados em consideração ao elaborar políticas de segurança. Entre essas normas estão a BS 7799 (elaborada pela British Standards Institution) e a NBR ISO/IEC 17799 (a versão brasileira desta primeira). A ISO começou a publicar a série de normas 27000, em substituição à ISO 17799 (e por conseguinte à BS 7799), das quais a primeira, ISO 27001, foi publicada em 2005.

Existem duas filosofias por trás de qualquer política de segurança: a proibitiva (tudo que não é expressamente permitido é proibido) e a permissiva (tudo que não é proibido é permitido).

Os elementos da política de segurança devem ser considerados:

- A Disponibilidade: o sistema deve estar disponível de forma que quando o usuário necessitar, possa usar. Dados críticos devem estar disponíveis ininterruptamente.
- A Legalidade.
- A Integridade: o sistema deve estar sempre íntegro e em condições de ser usado.
- A Autenticidade: o sistema deve ter condições de verificar a identidade dos usuários, e este ter condições de analisar a identidade do sistema.
- A Confidencialidade: dados privados devem ser apresentados somente aos donos dos dados ou ao grupo por ele liberado.

7.1 Políticas de Senhas

Dentre as políticas utilizadas pelas grandes corporações a composição da senha ou password é a mais controversa. Por um lado profissionais com dificuldade de memorizar varias senhas de acesso, por outro funcionários displicentes que anotam a senha sob o teclado no fundo das gavetas, em casos mais graves o colaborador anota a senha no monitor.

Recomenda-se a adoção das seguintes regras para minimizar o problema, mas a regra fundamental é a conscientização dos colaboradores quanto ao uso e manutenção das senhas.

- Senha com data para expiração

  Adota-se um padrão definido onde a senha possui prazo de validade com 30 ou 45 dias, obrigando o colaborador ou usuário a renovar sua senha.

- Inibir a repetição

  Adota-se através de regras predefinidas que uma senha uma vez utilizada não poderá ter mais que 60% dos caracteres repetidos, p. ex: senha anterior “123senha” nova senha deve ter 60% dos caracteres diferentes como “456seuse”, neste caso foram repetidos somente os caracteres “s” “e” os demais diferentes.

- Obrigar a composição com número mínimo de caracteres numéricos e alfabéticos

  Define-se obrigatoriedade de 4 caracteres alfabéticos e 4 caracteres numéricos, por exemplo:

  > 1s4e3u2s posicional os 4 primeiros caracteres devem ser numéricos e os 4 subsequentes alfabéticos por exemplo: 1432seus.

- Criar um conjunto com possíveis senhas que não podem ser utilizadas

  Monta-se uma base de dados com formatos conhecidos de senhas e proibir o seu uso, como por exemplo o usuário chama-se Jose da Silva, logo sua senha não deve conter partes do nome como 1221jose ou 1212silv etc, os formatos DDMMAAAA ou 19XX, 1883emc ou I2B3M4

- Recomenda-se ainda utilizar senhas com Case Sensitive e utilização de caracteres especiais como: @ # $ % & *

- Proibição de senhas que combinam com o formato de datas do calendário, placas , números de telefone, ou outros números comuns

- Proibição do uso do nome da empresa ou uma abreviatura

- Uma senha de Meio Ambiente, da seguinte forma: consoante, vogal, consoante, consoante, vogal, consoante, número, número (por exemplo pinray45). A desvantagem desta senha de 8 caracteres é conhecida a potenciais atacantes, o número de possibilidades que precisam ser testados é menos do que uma senha de seis caracteres de nenhuma forma.

Outros sistemas de criar a senha para os usuários ou deixar que o usuário escolha um de um número limitado de opções exibidas.

8 A Gestão de Riscos unida à Segurança da Informação

A Gestão de Riscos, por sua vez, fundamental para garantir o perfeito funcionamento de toda a estrutura tecnológica da empresa, engloba a Segurança da Informação, já que hoje a quantidade de vulnerabilidades e riscos que podem comprometer as informações da empresa é cada vez maior.

Ao englobar a Gestão da Segurança da Informação, a Gestão de Riscos tem como principais desafios proteger um dos principais ativos da organização – a informação – assim como a reputação e a marca da empresa, implementar e gerir controles que tenham como foco principal os objetivos do negócio, promover ações corretivas e preventivas de forma eficiente, garantir o cumprimento de regulamentações e definir os processos de gestão da Segurança da Informação. Entre as vantagens de investir na Gestão de Riscos voltada para a Segurança da Informação estão a priorização das ações de acordo com a necessidade e os objetivos da empresa e a utilização de métricas e indicadores de resultados.

9 Referências

[1]

[2] 'Meu amigo foi atacado por um hacker'; sistema da Microsoft tenta evitar roubo de senhas no Hotmail, acessado em 5 de maio de 2012

[3] Adrielle Fernanda Silva do Espírito Santo (2012). Segurança da Informação ICE.EDU. Visitado em 28/06/2015.

- Terpstra, John. *Segurança para Linux*. RJ: Elsevier, 2005. ISBN 85-352-1599-9

- Melhorar a usabilidade de Gerenciamento de senha com políticas de senha padronizados
- Claudia Dias, Segurança e Auditoria da Tecnologia da Informação, 2000, Editora: Axcel Books 142, ISBN 85-7323-231-9
- Brostoff, S. (2004). *Improving password system effectiveness*. Tese de Doutorado. University College London.
- Morris, R. & Thompson, K. (1979). Password security: a case history. *Communications of the ACM,* 22, 594-597.
- Sieberg, D. (2005). Hackers shift focus to financial gain. *CNN.com - Special Reports - Online Security*. Publicado em 26 de setembro de 2005.
- Smith, R.E. (2002). The strong password dilemma. *Authentication: From Passwords to Public Keys*. Chapter 6. Addison-Wesley.

10 Ligações externas

- Computer Security Institute (em inglês)
- CERT.PT (em português)
- CERT.br (em português)

11 Fontes, contribuidores e licenças de texto e imagem

11.1 Texto

- **Segurança da informação** *Fonte:* https://pt.wikipedia.org/wiki/Seguran%C3%A7a_da_informa%C3%A7%C3%A3o?oldid=43151569 *Contribuidores:* Jorge~ptwiki, PauloColacino, Manuel Anastácio, LeonardoG, Alancarv, Gbiten, Sr X, Nuno Tavares, Get It, NTBot, RobotQuistnix, Webcruiser, Leandromartinez, João Carvalho, Agil, Picoloto, OS2Warp, Adailton, Lijealso, YurikBot, Tmzani, Luís Felipe Braga, Arges, Tilgon, Profvalente, Marilene Morelli Serna, Leonardo.stabile, Amgauna, Davemustaine, Timor, Fabi polain, He7d3r, Girino, Belanidia, JSSX, Al3xander~ptwiki, JAnDbot, Alchimista, Antihacker, GostWriter, CSorin, BrWriter, Guilhermino1234, Carloscruz, BrWriter2, Augusto Reynaldo Caetano Shereiber, Clebermarques, Ghostwritter~ptwiki, RDantas2, Zaiosc, CarvalhoNonato, Luckas Blade, Joao Barbosa Jr, Tumnus, Gunnex, SCipriano, Weslevy, Teles, Natannael, Gerakibot, José1, RafaAzevedo, Alfredojr76, Ruy Pugliesi, Ebalter, Mpcorreia, !Silent, Vitor Mazuco, Fabiano Tatsch, MarlonAmorim, Luckas-bot, Panades, Salebot, Lépton, Darwinius, Thiago-Ruiz, Bssi, MastiBot, OnlyJonny, Euproprio, Marcos Elias de Oliveira Júnior, HVL, Alph Bot, Ripchip Bot, Crash Overclock, EmausBot, Savh, Reporter, Jbribeiro1, Stuckkey, WikitanvirBot, Jramio, Mariana S Souza, Colaborador Z, MerlIwBot, Rubens Luccas, Ariel C.M.K., Rlupiano, Zoldyick, Matheus Faria, Poison Whiskey, Fabiocax, Yuripobrasil, Moniquesorato, Negrijp, Legobot, Edsonborelli2012, ZeeQ, Victor R12, Nana Caê, Marcos dias de oliveira, Elthon Diego, Alissonmpereira, Jose.Alves IESF, Escritordiferente, ColdBloodOficial, Gabrieljborba, Michaeldfunivali, Diego Soleti e Anónimo: 205

11.2 Imagens

- **Ficheiro:Crypto.png** *Fonte:* https://upload.wikimedia.org/wikipedia/commons/f/f8/Crypto.png *Licença:* Public domain *Contribuidores:* Obra do próprio *Artista original:* Dev-NJITWILL
- **Ficheiro:Portal.svg** *Fonte:* https://upload.wikimedia.org/wikipedia/commons/c/c9/Portal.svg *Licença:* CC BY 2.5 *Contribuidores:*
  - Portal.svg

  Artista original: Portal.svg: Pepetps
- **Ficheiro:Wikibooks-logo.svg** *Fonte:* https://upload.wikimedia.org/wikipedia/commons/f/fa/Wikibooks-logo.svg *Licença:* CC BY-SA 3.0 *Contribuidores:* Obra do próprio *Artista original:* User:Bastique, User:Ramac et al.

11.3 Licença

- Creative Commons Attribution-Share Alike 3.0