Aten@ Revista Digital de Gestão & Negócios
UNIMES

A CRIPTOGRAFIA E SUA IMPORTÂNCIA NA ATUALIDADE

Aparecido Vicente[1]
Bernardo de Araújo
Luciano Magno Rocha
Vitor Henrique Ferreira de Lima Almeida
Elias Haddad[2]

RESUMO

Neste artigo desenvolvemos um estudo panorâmico sobre a Criptografia, descrevemos de forma rápida e objetiva o surgimento da mesma, bem como as passagens históricas mais importantes a seu respeito. Apresentamos de forma cronológica sua evolução, desde os primórdios do surgimento humano até os dias atuais. Também está presente aqui os sistemas criptográficos atuais, os algoritmos mais utilizados, além da importância da assinatura digital. Por fim sua acuidade no mundo contemporâneo, apontando patologias que podem prejudicar seu desempenho. Encerrando com sua perspectiva para o futuro.

Palavras-chave: Criptografia; Chaves; Simétrica; Assimétrica; Assinatura digital.

1- Discentes do curso Superior de Tecnologia de Gestão da Tecnologia da Informação
2- Docente do curso Superior de Tecnologia de Gestão da Tecnologia da Informação

1. INTRODUÇÃO

Surgindo no final dos anos 60, a internet fez revolução e trouxe para o mundo a agilidade e rapidez na transmissão de dados de forma precisa. Contudo a precisão de enviar e receber dados e/ou informações sigilosas é uma necessidade já ancestral ou remota há muito tempo atrás.

Em razão dessa imperatividade, a criptografia surgiu com o intuito de preservar e manter o sigilo dos dados, tornando-os "legíveis" somente ao emissor e receptor. Este artigo, realizado por meio da pesquisa bibliográfica, aborda a história, conceitos e características dessa ferramenta de grande importância para a segurança no mundo digital e que está presente no cotidiano da maioria das pessoas, mesmo sem que elas saibam.

2. O SURGIMENTO DA CRIPTOGRAFIA

> "No começo, as pessoas sussurravam. Outras escutavam clandestinamente. E, dessas primitivas e rudimentares origens, evoluiu uma das mais poderosas ferramentas da inteligência e uma das mais importantes técnicas de segurança do mundo atual."
>
> Adaptado de David Kahn
> (FERNANDES, 2009, p. 31 *apud* The Codebreakers, 1996)

Na evolução da espécie humana a preocupação em se "fazer" ou melhor dizendo "fluir" informação, é algo já abordado desde os primeiros remotos ancestrais, e nisso a espécie fez revolução. Ainda como "Homo sapiens" a troca de informação, técnicas ou conhecimento atravessou gerações a partir do momento que os mesmos começaram a emitir sons e articular a linguagem.

Posteriormente, as ideias começaram a sair do plano e passaram a ser esboçadas através de desenhos e pinturas em rochas e paredes das cavernas, por meio dessas se

registrou o elementar passo em informação impressa. Evoluindo para símbolos gráficos iniciando assim o primeiro meio organizado de informação (FERNANDES, 2009).

Inventada e aprimorada a escrita, logo após já se fez necessário o ato de ocultar a informação ou dissimular seu significado, a princípio de torna-la legível ou entendível somente aos fidedignos interessados, surgindo a Escrita Secreta por meio da esteganografia, codificação e a criptografia**.** A primeira consiste em esconder a mensagem em si, e as outras esconder seu conteúdo e/ou sentido.

A necessidade de proteger os canais e o conteúdo da comunicação das pessoas em uma comunidade surgiu então desde os primórdios da civilização. Os espartanos já faziam uso do conceito de escrita secreta, desenvolveram já naquela época (400 a.C.) uma forma de comunicação pessoal criptografada. A mensagem era escrita em uma tira de couro enrolada num bastão, ao desenrolar (do bastão) a mensagem era embaralhada, dessa forma somente enrolando-a novamente em um bastão de diâmetro semelhante que a mensagem poderia ser lida. Utilizando ainda da esteganografia a tira poderia ser disfarçada de cinto ou qualquer outra coisa, sendo dessa forma um método mecânico (abaixo), contudo engenhoso utilizado há muito tempo atrás.

Figura 1: Exemplo da Criptografia Espartana (Fonte: A criptografia e seu papel na segurança da Informação e das Comunicações (SIC) – Retrospectiva, atualidade e perspectiva - 2009).

Figura 2: Exemplo da Criptografia Espartana (Fonte: Criptografia - 2007).

O Imperador de Roma Júlio César (100 - 44 a.C.) também desenvolveu tal forma de comunicação com seus generais, através do deslocamento das letras do alfabeto, conhecida hoje por cifra de substituição. Considerando que o alfabeto era um ciclo fechado no qual após a última letra vem a primeira, para decifrar a mensagem, o receptor tinha que deslocar cada letra três vezes para a esquerda ou direita, revelando desta forma a mensagem original.

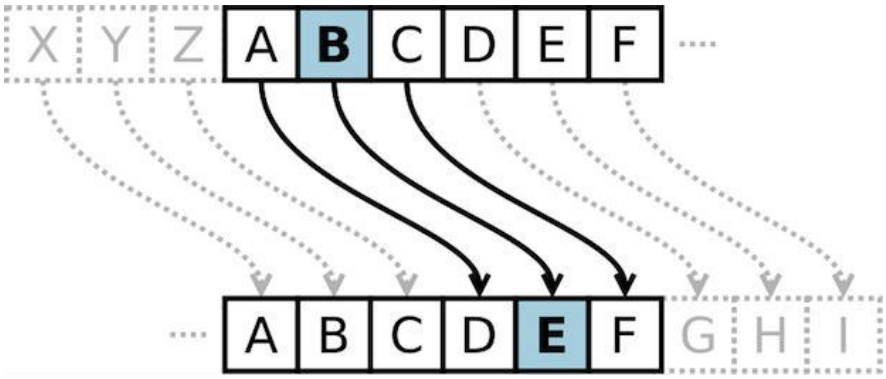
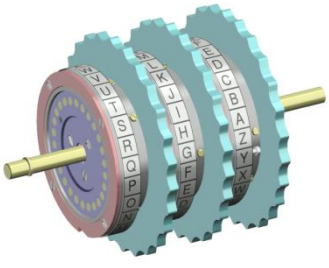


Figura 3: Código de César com chave de três unidades (Disponível em: http://www.techtudo.com.br/artigos/noticia/2012/06/o-que-e-criptografia.html - Acesso em 04/04/2016).

Com o passar do tempo esse recurso foi evoluindo e se tornando cada vez mais sofisticado, usado pelo exército Alemão na Segunda Guerra Mundial, por intermédio das "Máquinas Enigma". Tratava-se de uma máquina eletromecânica que trabalhava por meio de rodas ou rotores fixados no mesmo eixo, devido a isso o movimento contínuo dos rotores provocava diferentes combinações na criptografia, era utilizada para criptografar e descriptografar mensagens.



Respectivamente figuras 4 e 5: "Máquina Enigma" e "Rotores"

(Disponível em: https://pt.wikipedia.org/wiki/Enigma_(m%C3%A1quina) - Acesso em 02/04/2016).

Surgiu, então, a criptografia (do Grego: *kryptós*, oculto + *graphein*, escrever) muitos anos antes de Cristo, quase que simultaneamente com o surgimento da escrita. De uma forma clara, "criptografar" trata-se de um conjunto de técnicas que tem por objetivo codificar, embaralhar, tornando incompreensível uma determinada mensagem ou dado, de forma que somente o emissor e o receptor consigam acessá-las, evitando assim que um intruso possa interpretá-la. Para isso, várias técnicas foram utilizadas ao longo do tempo e outras permanecem até a atualidade.

Em termos literários, ao longo da história o desenvolvimento da criptografia passou por altos e baixos, sua produção era restrita até o ano de 1900. Todavia, em meados da Primeira Guerra Mundial, alguns fatos começaram a acontecer que propiciaram o desenvolvimento deste mecanismo de segurança. Após a guerra, as coisas começaram a tomar outro rumo. O exército e a marinha dos Estados Unidos se interessaram e começaram a trabalhar em segredo, conseguindo avanços muito significativos no assunto, contudo a divulgação ostensiva esvaeceu. Outros trabalhos e estudos a respeito da criptografia foram realizados, no entanto o controle militar era forte na época, desclassificando, então, os que surgiam.

2.1 SISTEMAS CRIPTOGRÁFICOS

Na computação, os métodos mais conhecidos envolvem o conceito de "chaves", que é baseado em um conjunto de *bits* em algum algoritmo que é capaz de codificar e decodificar informações ou dados. Dessa forma, o receptor deve ter uma chave compatível com a do emissor. Uma vez que não tendo o mesmo, não poderá extrair o conteúdo.

Os primeiros métodos existentes como a "Cifra de Júlio César", só utilizava um algoritmo de codificação (mono-alfabético), portanto o emissor só tinha que saber subtrair da mensagem três letras para decifrar. Nesse caso se um terceiro tomasse posse ou conhecimento desse algoritmo, também era capaz de decifrar. Esse método é conhecido por Chaves Simétricas.

Segundo Alecrim (2005), esse tipo de chave é mais simples, da qual o emissor e receptor fazem uso da mesma, isto é, para a codificação e descodificação é usada a mesma chave.

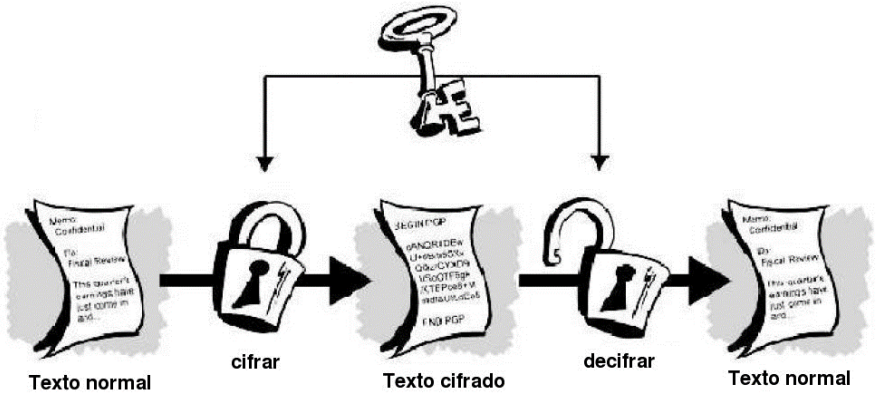


Figura 3: Chave Simétrica (Fonte: Criptografia – 2007).

No que se refere a esse tipo de algoritmo de chaves simétricas temos:

a) **DES (*Data Encryption Standard*):** criado em 1977, utiliza chaves de 56 bits**,** ou seja, sendo emissor e receptor elevado a 56 (*bits*), temos 72 quatrilhões de combinações que podem decifrar a informação. Um número extremamente alto, mas não para um computador potente.
b) **IDEA (*International Data Encryption Algorithm*):** criado em 1991, esse já tem base em chaves de 128 *bits*, possui estrutura semelhante ao DES, e sua implantação é mais fácil, considerando o anterior.
c) **RC (*Ron's Code ou Rivest Cipher*):** criando pela empresa RSA Data Security, tendo versões (RC2, RC4, RC5 e RC6) que variam de 8 a 1024 *bits*, muito utilizado por provedores de *e-mails*.

Portanto, chaves desse tipo não são apropriadas em caso de informações ou dados valiosos, já que a transmissão das chaves pode não ser muito segura e chegar a terceiros. Também devemos levar em conta que em episódio de muitos receptores ou entidades enredadas, o número de chave é muito grande, além de que o emissor e o receptor devem conhecer a mesma chave.

2.1.1 Criptografia Assimétrica

"Surge, então, o sistema de Criptografia Assimétrica ou de chave pública. Sistema em que o processo de cifração usa uma chave pública, mas em que o processo de decifração usa uma chave diferente, dita chave privada" (QUARESMA, 2007, p. 3).

Dessa forma, quando um emissor quiser receber dados criptografados deverá criar a chamada "chave pública" da qual disponibilizará para outros, que utilizarão dessa (pública) para enviar os dados criptografados. Sendo assim somente quem disponibilizar a chave inicialmente terá a possibilidade de desembaralhar o que recebeu.

Exemplificando para melhor compreensão, temos o emissor "A" que cria uma Chave Pública e distribui para os terceiros, "B" e "C". Quando "B" ou "C" quiserem mandar informação para "A", utilizarão da Chave Pública, da qual somente "A" terá a privada para decifrar. Caso "A" queira mandar algo criptografado para "B", deverá antecipadamente obter a chave pública fornecida pelo mesmo.

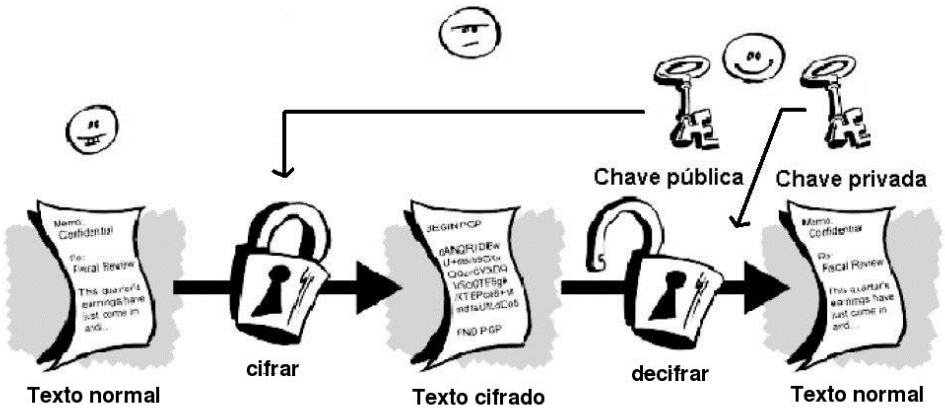


Figura 4: Chave Assimétrica (Fonte: Criptografia – 2007).

Abaixo alguns algoritmos que utilizam de "chave assimétrica":

a) **RSA (*Rivest, Shamir and Adleman*):** criado em 1977 nos laboratórios do MIT (*Massachusetts Institute of Technology*), sendo esse o algoritmo mais

utilizado das chaves assimétricas, através de números primos (aquele que só pode ser dividido por 1 e por ele mesmo). Como explica Alecrim:

> Dois números primos são multiplicados para se obter um terceiro valor. Porém, descobrir os dois primeiros números a partir do terceiro (ou seja, fazer uma fatoração) é muito trabalhoso. Se dois números primos grandes (realmente grandes) forem usados na multiplicação, será necessário usar muito processamento para descobri-los, tornando essa tarefa praticamente inviável. Basicamente, a chave privada no RSA são os números multiplicados e a chave pública é o valor obtido (ALECRIM, 2005).

b) **ElGamal:** Criado por Taher ElGamal, com intuito de se tornar mais seguro, este faz uso de problema matemático, conhecido até por logaritmo discreto, sendo frequentemente utilizado em assinaturas digitais.

2.1.2. Assinatura Digital

Atualmente, outro mecanismo de segurança também é utilizado para garantir a integridade de dados ou documentos. A chamada "Assinatura Digital" utiliza de criptografia assimétrica para sua execução. Assim como uma assinatura "a punho", a digital também só pode ser reproduzida de forma autentica por uma pessoa, entretanto todos tem acesso para verificar. A mesma também pode ser definida como:

> [...] um conjunto inforjável de dados assegurando o nome do autor que funciona como uma assinatura de documentos, ou seja, que determinada pessoa concordou com o que estava escrito. Tal procedimento também evita que a pessoa que assinou a mensagem depois possa se livrar de responsabilidades, alegando que a mensagem foi forjada (MORENO; DACÊNCIO; BARROS apud BURNETT, 2002).

Como saber se o documento foi alterado ou não? De forma simples, a partir do documento e sua respectiva assinatura digital é possível verificar a autenticidade do mesmo através do *Message Digest.* Executa então o *MD*, obtendo o *Hash* (pequeno

pedaço de dados) do documento a ser inspecionado, após decifra-se a assinatura digital utilizando da chave pública do remetente. Concluindo, a assinatura digital deve reproduzir/dar o mesmo *hash* que o do *MD* executado. *Message Digest* é usada para processar o documento, produzindo um pequeno pedaço de dados, chamado de *Hash*. Uma *MD* é uma função matemática que refina toda a informação de um arquivo em um único pedaço de dados de tamanho fixo (MOTA; CAVALCANTI, 1998)

Entretanto a partir disso só podemos saber se o documento foi modificado, não é possível saber o quanto e nem onde (MOTA; CAVALCANTI, 1998). Observe na representação abaixo, nela é utilizado o algoritmo de criptografia RSA de chave pública.

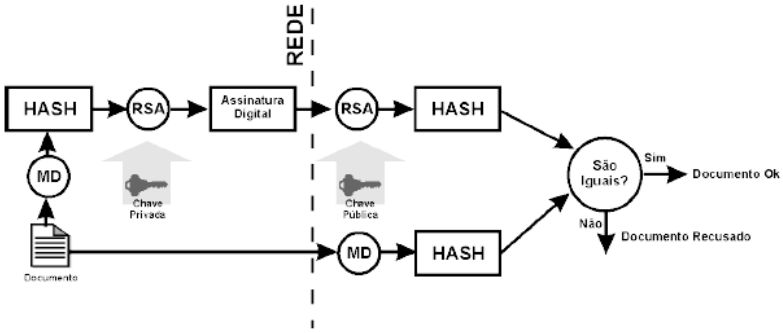


Figura 5: Autenticação Documento (Fonte: Um Estudo sobre Criptografia e Assinatura Digital – 1998)

"A assinatura digital também é valiosa, pois se pode assinar informações em um sistema de computador e depois provar sua autenticidade sem se preocupar com a segurança do sistema que as armazena" (MOTA; CAVALCANTI, 1998).

3. CRIPTOGRAFIA NA ATUALIDADE

Vivendo em mundo altamente conectado, a criptografia é indispensável para garantir a nossa segurança no meio, utilizamos de recursos que facilitam e muito o nosso dia-a-dia, a criptografia está presente em cada um deles. Quando precisamos fazer pagamento, consultar saldo, realizar transferências bancárias podemos de forma simples utilizar o smartphone. Através do aplicativo disponibilizado pelo banco, podemos entrar com os dados e gerenciar tudo a respeito, e é aí que a criptografia entra, a fim de que nossas informações não caiam em mãos erradas.

Todo e qualquer dado que utiliza ou esteja hospedado em rede, dispõe da criptografia para proteger e estar acessível somente as verdadeiras partes interessadas. A proteção vai, como citado anteriormente, de dados bancários, arquivos na nuvem, e-mails até a uma simples Mensagem SMS. O recurso então impede que informações sejam acessadas por intrusos e que os chamados "*Cyber* Crimes" aconteçam.

A criptografia também está presente nas redes sem fio, as senhas cadastradas são criptografadas a fim de permitir a conexão somente a quem inserir a senha correta. As notórias redes *Wi-Fi* disponibilizam de criptografia através de WEP, WPA e WPA2.

A rede social com maior número de usuários no mundo, o *Facebook*, conta com a criptografia na autenticação de seus usuários. Outras como a Apple, dispõe da criptografia densa para seus (aproximadamente) 800 milhões de *iPhones*, ela garante segurança nas mensagens (*iMessage*) trocadas em seus smartphones.

Recentemente um dos aplicativos mensageiros mais utilizados no mundo recebeu "criptografia de ponta a ponta". O *WhatsApp* liberou atualização para 1 bilhão de usuários, a criptografia foi ativada para todos, dessa forma a mensagem só poderá ser lida pelo real destinatário final. Ninguém será capaz de ler as mensagens, já que segundo a corporação "Nem nós mesmos".

Figura 6: Aviso WhatsApp (Disponível em: http://blogdoiphone.com/wpcontent/uploads/2016/04/WhatsAppEncrypt.jpg - Acesso em 09/04/2016).

A criptografia hoje é um assunto muito discutido mundialmente pelas autoridades. Para os usuários comuns, é de grande valia, contudo da mesma forma que protege as informações dos leigos, também "protege" os "vilões" que utilizam do recurso para esconder provas, ou "ficar no escuro". Segundo as autoridades os

criminosos estão começando a migrar para tais aplicativos, porque sabem que de uma forma ou de outra eles são segurados pela criptografia, então julgam ser uma "clássica e difícil opção".

Por outro lado, alguns casos pontuais não justificam essa investigação massiva em torno dos dados dos usuários, colocando desse modo a privacidade dos mesmos em risco, já que existem outras maneiras para se investigar um crime, e/ou descobrir criminosos. E que encontrar o equilíbrio entre investigar um crime e preservar a privacidade das pessoas é uma tarefa difícil ou talvez impossível.

CONSIDERAÇÕES

Sem dúvida, no mundo atual e digital que vivemos é imprescindível o uso da criptografia. Uma vez que sem ela nada do que usufruímos digitalmente poderia laborar, como os serviços bancários na palma da mão, comércio online, privacidade nas milhares de mensagens trocadas diariamente.

Contudo algumas ocasiões estão colocando em risco esse recurso indispensável para o nosso dia-a-dia, em razão da criação de leis ou brechas para investigações criminais. Já não basta sermos vigiados constantemente nos cruzamentos, shopping centers, praças... também estamos sendo invadidos digitalmente, além da grande rede de computadores que formamos que já se encontra totalmente controlada e vigiada.

Desse modo não nos restam dúvidas de que a nossa privacidade está entrando na extinção, sendo atacada cada vez mais, e o pior, esse processo parece ser irreversível. Em verdade, a nossa privacidade só era total quando não existia a internet, hoje não é mais.

REFERÊNCIAS

CASSIA, A. *Criptografia***.** Disponível em: <http://www.estudokids.com.br/criptografia/>. Acesso em: 15 de abr. 2016.

DANTAS, T. *Criptografia*. Disponível em: <http://mundoeducacao.bol.uol.com.br/informatica/criptografia.htm>. Acesso em: 15 de abr. 2016.

FERNANDES, E. C. *A criptografia e seu papel na segurança da Informação e das comunicações (sic) – Retrospectiva, atualidade e perspectiva.* 2009**.** 84 f. Trabalho de Conclusão de Curso (Especialização). Universidade de Brasília – Instituto de Ciências Exatas, Brasília/DF, 2009.

MORENO, E. D.; DACÊNCIO, F. P.; BARROS, R. C. Conceitos de Segurança de Dados e Criptografia. In: MORENO, E. D.; DACÊNCIO, F. P.; BARROS, R. C. *Criptografia em Software e Hardware*. 1 ª Edição. São Paulo: Novatec Editora, 2004. p. 21 – 42.

MOTA, F. A. T.; CALVACANTI, R. M. *Um Estudo sobre Criptografia e Assinatura Digital.* Disponível em: <http://www.di.ufpe.br/~flash/ais98/cripto/criptografia.htm>. Acesso em: 12 de abr. 2016.

PISA, P. *O que é Criptografia?* Disponível em: <http://www.techtudo.com.br/artigos/noticia/2012/06/o-que-e-criptografia.html>. Acesso em: 10 de abr. 2016.

SCHUNCKE, A. *Quais os principais tipos de criptografia?* Disponível em: <https://www.oficinadanet.com.br/post/9424-quais-os-principais-tipos-de-criptografia>. Acesso em: 08 abr. 2016.

YOSHIDA, Y. *Segurança, Criptografia, Privacidade e Anonimato.* Disponível em**:** **<**https://www.ime.usp.br/~is/ddt/mac339/projetos/2001/demais/elias/>. Acesso em: 10 de abr. 2016. Universidade Metropolitana de Santos (Unimes) Núcleo de Educação a Distância - Unimes Virtual.

COSTA, C**.** *Quatro coisas que mudam com a criptografia no WhatsApp – e por que ela gera polêmica.* Disponível em: <http://www.bbc.com/portuguese/noticias/2016/04/160406_whatsapp_criptografia_cc>. Acesso em: 02 abr. 2016.

Elias Salim Haddad Filho

Mestre em Gestão de Negócios e Bacharel em Administração. Professor de Marketing e de Administração das Micro e Pequenas Empresas no Núcleo de Ensino a Distância da UNIMES - Universidade Metropolitana de Santos, no curso de Administração. Autor do livro Qualidade de Vida e Desenvolvimento Econômico Sustentável em Santos. Áreas de interesse e pesquisa: qualidade de vida urbana, desenvolvimento dos municípios, marketing de cidades e marketing de varejo.

Para citar este trabalho:

VICENTE, Aparecido**; ARAÚJO,** Bernardo de**; ROCHA,** Luciano Magno**, ALMEIDA,** Vitor Henrique Ferreira de Lima**; HADDAD,** Elias**. A CRIPTOGRAFIA E SUA IMPORTÂNCIA NA ATUALIDADE . Revista Atena@ .Vol.1 – Número 0 – AGOSTO 2016 . Disponível em:**

http://periodicosunimes.unimesvirtual.com.br/index.php?journal=gestaoenegocios&page=index