# SEGURANÇA DA INFORMAÇÃO

MILANI, T. G.[1,2, 3]

[1]Dicente MBA em Tecnologia da Informação com Ênfase em Segurança da Informação - Centro Universitário Hermínio Ometto – UNIARARAS, Araras, SP.; [2]Dicente MBA em Gestão de TI – Anhnaguera Educacional - Rio Claro, SP; [3]Professor PRONATEC Anhnanguera Educacional - Rio Claro;

http://consultoriaemti.wix.com/thiago
thiagogmilani@gmail.com

## RESUMO

Segurança da informação hoje em dia é algo que quase todas as empresas estão se preocupando, com o grande crescimento da tecnologia e o uso de internet e diversos aparelhos e em qualquer lugar esta cada vez mais fácil ser infectado por um vírus, virar um “zumbi” na rede mundial de computadores, ou até mesmo ser vítima de engenharia social. Este artigo fala brevemente sobre segurança da informação, e os principais conceitos. Segurança é proteger a integridade dos dados confidencias da empresa ou instituição, com isso a segurança da informação é sustentada sob três pilares; Prevenir, Detectar, Recuperar. Prevenir se baseia em impedir eventos de segurança, como invasão, roubo e violação de políticas de segurança. Detectar, baseia-se em como, quando e de que forma foi feito uma invasão. Recuperar é a tarefa de avaliar os danos causados em um sistema, recuperando-os para a sua operação normal. A segurança também pode ser definida com as seguintes características, Confiança, onde consiste em proteger um dado contra a ruptura do fato de ser confidencial, para isso pode ser usado técnicas como criptografia. Autenticidade, onde é a capacidade de se autenticar que apenas as partes envolvidas estão realmente acessando os dados. Integridade, é a garantia de que a informação não sofreu nenhuma alteração indevida durante o trajeto do dado. Disponibilidade é a capacidade de sempre estar disponível quando necessário em qualquer uma das partes. E o não repúdio, é o que garante que o envio de informação original não seja negada pela outra parte interessada. As ameaças podem vir de qualquer parte do mundo, e podem ser intencionais ou não-intencionais, as intencionais são aquelas no qual existe uma ou mais pessoas maliciosas querendo prejudicar e causar danos a outra, já a ameaça não intencional é aquela no qual um serviço acaba ficando indisponível por meio de uma grande quantidade de acessos, como por exemplo uma liquidação muito grande em um site de comprar, ou uma inscrição a uma concurso muito concorrido, que devido a uma grande quantidade de pessoas querendo se inscrever, ou efetuar a compra, acabam sobrecarregando o servidor não intencionalmente, e assim afetando a disponibilidade do mesmo. As vulnerabilidades são falhas que podem ser exploradas por programas maliciosos como *malware*. Risco é a ameaça de ter uma vulnerabilidade que possa ser explorada e causar perda e danos. A segurança da informação também engloba o ambiente físico no qual dependendo de a política de segurança pode requerer permissões de acesso, ou até mesmo de filmagem ou para tirar fotografias. Além disso a evolução nos trouxe a biometria como sistema de segurança mais rápido e difícil de ser

corrompido, no qual pode ser de vários tipos, biometria digital onde é capturado a impressão digital e convertida em código que não pode ser repetido por nenhuma outra impressão digital, existe a biometria da ires, que é a leitura da retina dos olhos, a biometria facial, que é a leitura do formato do rosto, entre outras. Para que tudo isso tenha uma segurança maior ainda, e não seja de fácil acesso os códigos reais e senhas, existe a criptografia, que pode ser de pois tipos principais, a criptografia simétrica, que utiliza uma única chave de criptografia tanto para criptografar o arquivo como decriptografa-lo quando necessário, e a criptografia assimétrica, na qual utiliza duas chaves, o conceito de chave pública e chave privada, na qual a chave pública é utilizada para a criptografia do arquivo, e como o próprio nome diz, é pública, e a chave privada que é utilizada para de criptografar o arquivo, no qual apenas o próprio domo deverá ter, e não passará para ninguém, assim o segredo para abrir o arquivo e ver seu real conteúdo será apenas dele, criando uma maior segurança para o arquivo que estará sendo transferido. Uma das maneira de se evoluir a segurança da informação em uma empresa é com uma política de segurança bem elaborada e com uma conscientização dos de mais colaboradores do quão importante ela é, nessa política de segurança deve ser especificado todas as diretrizes de segurança, desde quem tem acesso as salas onde estão os equipamentos, as pessoas responsáveis pela manutenção dos equipamentos, até as obrigações e direitos do usuário de computador, seja ele de qual setor for, e caso tenha diferenças de permissões entre departamentos devem ser especificadas também. Com isso podemos ver que a segurança da informação é ampla e se não for bem estudada e planejada pode acabar causando mais problemas do que solucionando-os, além de criar vulnerabilidades ao invés de impedi-las, uma segurança bem organizada e gerenciada constantemente, pode chegar a reduzir muito os problemas de empresas, porém quando falamos de tecnologia da informação podemos contar sempre com evoluções constantes.

## REFERÊNCIAS BIBLIOGRÁFICAS


**THOMAS, TOM.** Segurança de Redes. Primeiros Passos. Rio de Janeiro: Editora Moderna, 2007;

**TANENBAUM, Adrew S.** Redes de Computadores. Rio de Janeiro: Editora Campus, 2003, 4ed;

**CERT.** Cartilha de Segurança na Internet. Disponível em: http://cartilha.cert.br/ Acesso em: 04 de abril de 2015;

**NAGIOS.** Disponível em: http://nagios-br.com/ Acesso em 04 de abril de 2015;

**CARVALHO, Guilherme Pires Sales de; SANTOS, Thiago Monte dos.** Biometria por voz. Disponível em: http://www.gta.ufrj.br/grad/09_1/versao-final/impvocal/biometria-vozint.html. Acesso em: 04 de abril de 2015;

**FERREIRA, Matheus F. T.; et. All.** – Análise de Vulnerabilidade em Sistemas Computacionais Modernos, Conceitos, Exploites e Proteção. Disponível em : http://www.fpf.br/download/2012_analise_vulnerabilidades_em_sistemas.pdf Acesso em: 04 de abril de 2015;

**MILANI T. G**. Honeypot para detecção e contenção de ataques e bootnets, Disponível em: http://www.profissionaisti.com.br/2014/08/honeypot-para-deteccao-e-contencao-de-ataques-e-botnets/ Acessado em: 04 de abril de 2015.