

NOME: LETÍCIA DA SILVA ZARBIETTI COÊLHO

TÍTULO: SEGURANÇA DA TECNOLOGIA E DA INFORMAÇÃO: COMO PROTEGER SEUS DADOS

AUTORES: LUCIANO MAGNO ROCHA, LETÍCIA DA SILVA ZARBIETTI COÊLHO , JULIANA MACHADO CARVALHO, FRANCISCO ROMANO JUNIOR, MARCELO OLIVEIRA SILVA, LUCIANO MAGNO ROCHA, LETÍCIA DA SILVA ZARBIETTI COÊLHO

AGÊNCIA FINANCIADORA (se houver): NÃO POSSUI

PALAVRA CHAVE: SEGURANÇA, VULNERABILIDADE, ATAQUE, HACKER

RESUMO

Quando se fala em segurança de sistemas as pessoas associam o tema a hackers e vulnerabilidade, e muitas empresas acreditam que um bom antivírus aplicado no meio tecnológico é suficiente para proteger as informações da empresa. Veremos que existem uma série de ameaças que podem comprometer o seu sistema. Com o intuito de conscientizar as pessoas da importância da segurança, realizei uma pesquisa demonstrando que somente o uso de um antivírus, não é o suficiente para garantir a segurança da informação, mas que existe uma série de ameaças, que as pessoas e as empresas precisam se proteger. Este artigo, tem como base a pesquisa bibliográfica à luz de LEVY (2000), SÊMOLA (2003), entre outros, como procedimento metodológico para construção do conhecimento, relacionado a segurança da informação, cujo objetivo é demonstrar os tipos de ameaças existente. A ameaça pode ser definida como ação, acontecimento ou entidade que possa agir sobre um ativo, processo ou pessoa, através da vulnerabilidade gerando um determinado impacto. As ameaças são divididas em grupos e classificada conforme sua intencionalidade, sendo elas: Ameaças naturais; Ameaças involuntárias; Ameaças físicas; Ameaças Voluntárias. Para uma empresa ter suas informações seguras, o mais adequado é contratar um técnico de informática, para corrigir a vulnerabilidade do seu sistema, reparando falhas ou brechas, para que os dados fiquem seguros. Podemos concluir, que nenhum sistema é totalmente seguro, e que um antivírus é apenas um item na segurança para proteger os dados, não basta contar apenas com essa ferramenta. Como cada caso é um caso, o ideal é que haja um plano para combater o problema. Usuários residenciais, devem procurar um técnico de confiança, para manter suas informações segura, e as empresas, precisão de uma equipe de segurança bem preparada, que conheça bem a estrutura das aplicações da empresa e conte com ferramentas computacionais adequadas para que sejam eficientes no combate aos ataques.