

# Segurança da Informação

Fernando Alberto, Otavio Bianchi, Ronni Cleverson Duarte, Orlei José Pombeiro

Grupo de Pesquisa em Informática, Bacharelado em Sistemas de Informação,  
Sociedade Paranaense de Ensino e Informática - Faculdades SPEI  
Fone(41)3321-3131, Fax (41)3321-3142

[billiegdjoe@gmail.com](mailto:billiegdjoe@gmail.com), [otaviobianchi@hotmail.com](mailto:otaviobianchi@hotmail.com), [ronnibom@ig.com.br](mailto:ronnibom@ig.com.br), [orlei@spei.br](mailto:orlei@spei.br)

**Resumo** – A informação, os processos de apoio, sistemas e redes são importantes ativos e também, estratégicos para os negócios. Confiabilidade, integridade e disponibilidade, são características chave para a segurança da informação, é através dessas características que é possível preservar a competitividade, o faturamento, a lucratividade, o atendimento aos requisitos legais e a imagem da organização no mercado. As organizações estão extremamente preocupadas com a segurança nos sistemas de informação e redes de computadores. É necessário garantir a confiabilidade e segurança de suas transações e combater os ataques causados por vírus, hackers e phishings, que estão se tornando cada vez mais comuns, mais ambiciosos e incrivelmente mais sofisticados.

**Palavras-chave:** Segurança da informação, criação de senhas, estratégias de segurança.

## Introdução

Com o crescimento da globalização, o acesso à informação está mais fácil. O reflexo deste novo panorama traduz-se em episódios cada vez mais frequentes de saques eletrônicos indevidos, clonagem de cartões de crédito, acesso a bases de dados confidenciais, dentre inúmeras outras ameaças.

A segurança da informação vem sendo tema de grande debate neste novo milênio. As organizações estão buscando soluções práticas e efetivas, que possam trazer otimização de suas atividades, mas ao mesmo tempo segurança em operar seus mecanismos de trabalho.

Existem técnicas de como escapar ou evitar os ataques mais comuns à informação, fazendo um paralelo entre os problemas, sintomas, prevenções e soluções.

## Navegação pela Internet

A explosão dos ataques online está longe de esfriar e parece haver cada vez menos lugar para correr.

De acordo com a consultoria Sophos, o ano passado teve um aumento de 48% na atividade dos chamados malwares, que englobam toda gama de praga virtual [1].

O problema não é só dos “vírus”. Somente em 2005 foram encontradas 5198 vulnerabilidades diferentes em Sistemas Operacionais (S.O.), como Windows, Mac-OS X e Unix/Linux, e segundo o Computer Emergency Readiness Team (Cert), nem todos foram corrigidos [1].

Engana-se quem imagina que esse tipo de problema é somente do exterior. Aqui no Brasil as fraudes on-line aumentaram quase 600% em 2005, segundo dados do Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (Cert.br) [1].

Mais esse tipo de problema não está disponível somente para PC's e seus S.O.. As pragas para celulares, já atingia o número de 87, em setembro de

2005 segundo a F-Secure. Assim como os Vídeo-Games Nintendo DS e Playstation Portable, eles também já têm seus vírus (caso sejam infectados, não servem mais para nada) [1].

## Como criar senhas seguras

Senha fácil é a porta de entrada para ataques bem sucedidos por pessoas mal-intencionadas. E enquanto a biometria não se torna uma realidade, temos que garantir que a velha e boa senha continue protegendo as informações.

Porém, mesmo sendo antiga, ela deve estar sempre atualizada. Antigamente, as senhas consideradas fortes eram as que tinham 6 caracteres numéricos, mais com o avanço da tecnologia, hoje em dia isso é muito fácil de ser quebrada.

Na Tabela 1: Como criar senhas, existem dicas de como se deve e como não se deve criar uma senha.

Também pode ser usada a criatividade, utilizando-se da primeira letra de uma frase unida com a pontuação, ou ainda, usar software que geram senhas aleatórias para o usuário. O que não pode ser esquecido, é que 80% dos problemas de segurança que temos, são causadas por senhas “fracas”, conforme estimativa do CERT [2].

Outra dica é usar uma senha com, no mínimo, 8 caracteres, tendo sempre nela, obrigatoriamente, uma letra, um número e um caractere especial como: @, %, &, ou +, e se usar uma palavra apenas, escreve-la de forma incorreta, exemplo: No momento em que for criada, troque o “A” por “4”, “L” por “1” e adicione um caractere especial no início, meio e final, como um “@”. Se fosse escolhida a palavra “casamento”, escrevendo errado, ela ficaria “#k4sa^m3nt0&”. Isso já dificultaria bastante os aplicativos *brute force*[2], programas para decifrar senhas, usando todas as alternativas para descobrir-la[2].

Outra regra para manter as senhas mais seguras, é troca-las regularmente. As mais importantes, como as de Internet Banking, devem ser alteradas

mensalmente, assim garantindo a segurança do acesso. Outra dica, bastante fácil ser aplicada, é quando acessar o Banco on-line, na hora de digitar-la, escreva-a totalmente errada na primeira tentativa de acesso, se por acaso não der nenhum erro de senha invalida, significa que é um site falso. Saia imediatamente dele e comunique o seu banco o mais rápido possível.

Tabela 1: Como criar senhas

O que fazer com a sua senha	O que NÃO fazer com a sua senha
Misture letras em maiúsculo e minúsculo além de números e caracteres especiais	Não utilize nenhuma palavra do dicionário, mesmo em outra língua, acrônimos e abreviações.
Utilize caracteres alfanuméricos com pontuação quando suportado pelo sistema.	Não use seu nome, apelido ou suas iniciais como base para criação de senha.
Utilize mais letras em maiúsculo do que apenas na primeira posição.	Não utilize nenhuma variação do seu login de rede.
Troque obrigatoriamente sua senha se suspeitar de algum vazamento ou do comprometimento do seu sigilo.	Não utilize nenhuma outra informação sobre você que possa ser facilmente obtida. Incluindo nome de animais de estimação, números de telefone, marca de automóveis, nome de ruas.
Forme uma senha aparentemente randômica, sem q ela tenha significado lógico.	Não utilize seqüências de teclas do teclado.
Forme uma senha que se possa digitar rapidamente sem ter que olhar no teclado.	Não utilize datas ou combinação de datas como base para formação e senhas.
Troque sua senha regularmente. A frequência deve acompanhar a criticidade do bem protegido.	Não utilize senhas formadas somente por números ou caracteres alfanuméricos, quando o sistema permitir.
Evite associações quando forma de senha. Forte é a senha que não se consegue descobrir por dedução.	Não use exemplo de senhas mencionadas em livros sobre segurança ou qualquer outra literatura, por mais forte que possa parecer.
Memorize a senha, mais se tiver de escrever, escreva apenas algo que faça lembra-la.	Não escreva as senhas em papeis, notas, calendários ou em ambiente on-line se outros usuários puderem acessar.
Use pelo menos 8 caracteres, aumentando preferencialmente para 10.	Não compartilhe contas de acesso e senhas e não revele sua senha para ninguém.

Fonte: Marcos Sêmola [2]

### Phishing: conto do vigário digital

“Não é delírio dizer que a versão digital do ‘conto do vigário’ é o phishing” [3]. Além disso, com o avanço da Internet, os golpes ficaram mais vastos e

perigosos, migrando das cidades do interior para qualquer micro conectado a Web.

Para funcionar, o cracker joga uma isca (daí o nome phishing), como um e-mail de um banco idêntico ao original, para que o usuário baixe o sistema malicioso que envia tudo o que ele digitar em seu PC ou envia informações sigilosas pela Web, como senhas de banco. E um aspecto que ajuda esse tipo de crime é a curiosidade do usuário.

O pior de tudo, é que esse tipo de praga não traz códigos maliciosos integrado a ele, o próprio usuário tem que clicar e instala-lo sendo enganado pela engenharia social.

Portanto, para evitar mais esse incomodo, é o usuário que tem que ficar atento.

### Vírus e Pragas

Os vírus foram os primeiros a começar o pânico na Internet. A infecção acontece geralmente por e-mail, que contem um arquivo malicioso, anexado a ele, enviado para o usuário.

Mesmo tendo diminuído com o tempo, esse tipo de recurso ainda é bastante usado, e para evitar a contaminação, o usuário deve seguir 3 dicas importantes: Ter sempre um antivírus atualizado, nunca abrir arquivos de pessoas desconhecidas ou que achar estranho e ter um firewall no seu PC. Assim ele evita, porém, não soluciona totalmente, a infecção.

Fora os aplicativos, todas as velhas dicas sobre segurança continuam valendo, “É até meio clichê, mas tem que desconfiar de e-mails de pessoas desconhecidas e ter cuidado ao visitar sites pouco famosos” [4].

### Alem do e-mail

Porém, não são só os e-mails que podem infectar um PC. As redes P2P de troca de arquivo e as paginas Web também podem esconder códigos maliciosos.

“Quem baixa musica em programas de compartilhamento deve estar bem mais atento. É fácil baixar uma canção com um vírus integrado, sem que se desconfie” [4]. Essa técnica é conhecida como *morphin*, em que o Craker acopla um vírus no arquivo em MP3.

Com uma simples navegação, o usuário pode ser infectado. Ao contrario dos ataques tradicionais, a praga contamina o PC sem que o usuário o instale. Para esses casos, exige medidas um pouco mais drásticas. “É necessário observar o cadeado que o Internet Explorer mostra sempre que se visita uma pagina segura e nunca clicar em links desconhecidos” [4].

Outra ameaça, que também se instala sem que o usuário saiba, é o Spyware, que tem a função de roubar as senhas e dados pessoais, fazendo com que aumente de 3 para 4 dicas de segurança importante: instalar um software anti-Spyware.

O CISO (Chief Information Security Officer) da Universidade da Geórgia (EUA), Stan Gatewood, em parceria com o Computerworld, reuniu os principais passos para construir – ou mesmo reestruturar – o

departamento de segurança da informação da sua empresa. [5]

Conheça 13 dicas para criar sua estratégia de segurança:

1. Identifique um executivo líder. Um executivo patrocinador precisa defender a nova estratégia do programa de segurança.

2. Selecione uma pessoa principal. O CISO ou outro líder de segurança devem gerenciar diariamente as atividades.

3. Defina ou priorize os objetivos. Tente amarrar os objetivos de negócio aos de segurança.

4. Estabeleça um mecanismo de revisão. Um processo revisto pela diretoria, por executivos de tecnologia da informação, segurança física, recursos humanos, jurídico, auditoria e pela área de segurança da informação avaliará e aprimorará as iniciativas.

5. Estime o estado corrente da segurança. Considere política, processos, sugestões, padrões, tecnologias existentes (hardware e software), treinamento e educação.

6. Estabeleça – ou restabeleça – a organização da segurança. O grupo deve ter o foco na segurança das informações, não só as limitações das tecnologias que possui.

7. Revise a posição existente e desenvolva novas de acordo com as necessidades. Isso pode incluir uma política aceitável e configuração de segurança mínima para qualquer equipamento da rede.

8. Monte times de implementação. Coloque juntos grupos com funções complementares, com funções técnicas e de negócio para orquestrar os planos as novas políticas, iniciativas, ferramentas e processos.

9. Tenha um executivo da diretoria de segurança revisando os planos. Este grupo deve considerar o orçamento, tempo de execução e prioridades.

10. Revise as possibilidades técnicas. Isto pode ser feito por um técnico de segurança que represente o escritório do CIO e do CTO, mais o pessoal de operações, serviços de produção e suporte.

11. Determine, faça a programação, execute e discute o que pode ser feito e entregue. Dê claras responsabilidades individuais e de grupo.

12. Coloque toda a equipe de trabalho no plano estratégico. Cada um do departamento de segurança deve estar apto a introduzir e explicar os objetivos do plano de segurança e detalhar como os projetos estão contribuindo para a meta da empresa.

13. Mensure resultados com métricas e estas métricas de segurança de TI devem estar baseadas em objetivos que terminem em decisões certas e melhorias de negócio

## Resultados

Através das práticas aqui discutidas, é possível estar mais protegido quanto aos mais diversos tipos de ameaças digitais. Algumas delas requerem um estudo aprofundado de como a informação está estruturada, já outras requerem apenas simples medidas que podem ser

tomadas sem maiores impactos em nossa vida, como mudar uma senha a cada 3 meses ou quando for conveniente.

Nota-se que a maioria dos casos de infecção acontece por falha do usuário ao não tomar cuidado ao ver e-mails ou deixar o antivírus desatualizado ou por falhas na política de segurança das empresas, aonde os invasores se aproveitam de técnicas de engenharia social para conseguir as informações que necessita. Já nos casos de roubo de senhas, normalmente são causados por programas maliciosos instalados no computador da vítima sem que a mesma tenha consciência disso.

## Conclusões

Por mais que os melhores softwares estão instalados nos PC's, sempre manter a atenção em relação a segurança da informação é fundamental, pois, uma boa parte das pragas que infectam os sistemas, são pegadas simplesmente pela falta de cuidado ao ver e-mails ou usar o Internet Banking.

A frase “É melhor prevenir do que remediar” cabe muito bem quando o assunto é a prevenção, ou seja, tomar cuidado ao visitar um site desconhecido, ver e-mail de pessoas estranhas ou digitar senhas em lugar que não são seguros como lan- house..

## Referências

[1][http://idgnow.uol.com.br/seguranca/2006/02/24/idgnoticia.2006-02-24.2994903364/IDGNoticia\\_view](http://idgnow.uol.com.br/seguranca/2006/02/24/idgnoticia.2006-02-24.2994903364/IDGNoticia_view)

[2][http://idgnow.uol.com.br/seguranca/firewall/idgcoluna.2006-08-18.5368218714/IDGColuna\\_view](http://idgnow.uol.com.br/seguranca/firewall/idgcoluna.2006-08-18.5368218714/IDGColuna_view)

[3][http://idgnow.uol.com.br/seguranca/2006/02/24/idgnoticia.2006-02-24.7680983941/IDGNoticia\\_view](http://idgnow.uol.com.br/seguranca/2006/02/24/idgnoticia.2006-02-24.7680983941/IDGNoticia_view)

[4][http://idgnow.uol.com.br/seguranca/2006/02/24/idgnoticia.2006-02-24.5481078781/IDGNoticia\\_view](http://idgnow.uol.com.br/seguranca/2006/02/24/idgnoticia.2006-02-24.5481078781/IDGNoticia_view)

[5][http://idgnow.uol.com.br/seguranca/2006/09/18/idgnoticia.2006-09-18.8251518357/IDGNoticia\\_view](http://idgnow.uol.com.br/seguranca/2006/09/18/idgnoticia.2006-09-18.8251518357/IDGNoticia_view)

[6][http://idgnow.uol.com.br/seguranca/2006/02/24/idgnoticia.2006-02-24.1177261050/IDGNoticia\\_view](http://idgnow.uol.com.br/seguranca/2006/02/24/idgnoticia.2006-02-24.1177261050/IDGNoticia_view)