

---

## Internet sem limites compromete produtividade de empresa

Até pouco tempo, o máximo que um funcionário podia fazer contra a empresa era estender-se no cafezinho, criar intrigas internas, conversar ao telefone com amigos e familiares.

Com o advento da internet e sua ampla difusão nas empresas, os funcionários passaram a ter contato ilimitado com o mundo externo. Surgiu a figura do *Cyberslacking*: sujeito que utiliza intensamente a internet no ambiente de trabalho para fins pessoais.

Este “sujeito” corresponde a 90% dos funcionários das empresas, segundo pesquisa da Vault.com. E mais, 15% ultrapassam as 2 horas diárias.

As conseqüências são graves como a queda no rendimento profissional, o aumento de consumo da banda de internet, a contaminação dos computadores por vírus, aumento da vulnerabilidade e a responsabilidade legal da empresa sobre os atos do funcionário, enfim, perda de dinheiro e ganho de preocupações.

A responsabilidade legal é, sem duvida, a conseqüência mais grave de todas. Justifico: se os problemas com queda de rendimento, consumo de banda e contaminação podem ser controlados por chefes atentos e softwares específicos, a responsabilidade fica tomada de abstratividade e imprevisibilidade.

Abstrata porque não há resultado material perceptível e imediato; imprevisível por depender de conduta futura e incerta.

Como exemplo, poderíamos aduzir que o aumento de banda e a queda de desempenho são controláveis, já se um funcionário irá maltratar um cliente via e-mail é imprevisível e praticamente incontrolável.

Temos ainda a norma, que entre outras destaco:

**“Art. 932. São também responsáveis pela reparação civil:**

III – o empregador ou comitente, por seus empregados, serviçais e prepostos, no exercício do trabalho que lhes competir, ou em razão dele”

E a tecnologia também pode conspirar em favor do funcionário. Tecnicamente explicando, as empresas utilizam uma única conexão e as compartilham para os funcionários, ou seja, existe um IP publico (visível para todo o mundo) e vários inválidos (utilizados e conhecidos somente internamente).

Desta forma, todos os e-mails, acessos, e interações com o mundo externo estão relacionados com o IP publico da empresa, sendo por vezes, impossível identificar quem dentro da empresa é o autor de determinado acesso.

Ademais temos os limites ao poder de direção do empregador. Quem pensa que estes problemas podem ser evitados com uma rígida monitoração eletrônica do funcionário, como por exemplo a leitura dos e-mails enviados e recebidos, terá de enfrentar as garantias fundamentais estabelecidas na Constituição e a

divergência jurisprudencial.

E com isso a problemática está criada. Como evitar que informações confidenciais vazem? Como evitar ameaças, invasões e fraudes? Como transferir a responsabilidade para o funcionário?

Uma ótima solução é implementar a norma NBR ISO 17799, que se trata de uma série de procedimentos e regras que praticamente esgotam o tema política de segurança. Esta implementação é feita em conjunto por especialistas em tecnologia e direito eletrônico.

Contudo, pode não ser uma solução palpável para pequenas e médias empresas, em função do seu custo. Vale a ressalva, o gasto com precaução é menor que com reparação.

Para aqueles que leram este texto em busca de alguma orientação, faço algumas observações que podem ser tomadas de plano sem maiores esforços.

1- Desenvolva uma política de utilização dos meios eletrônicos, envolva as áreas de TI e Segurança, RH e Jurídico. Divulgue amplamente estas políticas.

2- Mantenha controle dos acessos e armazene os “logs”.

3- Promova Programas de conscientização.

4- Armazene os e-mails enviados e recebidos, posteriormente poderão ser utilizados em favor da empresa em processos judiciais e administrativos.

5- Leia as normas de segurança (NBR ISO 17799 entre outras).

6- Participe de fóruns, debates e palestras sobre o tema.

7- Desative recursos desnecessários, como drivers de disket e cd-rom, caixas de som etc...

8- Desenvolva contratos de confidencialidade com os funcionários.

9- Conte com o apoio e orientação de profissionais e empresas especializadas.

10- Esteja atento, a maior ameaça pode estar dentro da empresa.

Esteja certo que a má utilização da internet não é um mero problema de disciplina, o **International Data Corporation** (www.idc.com) indica que a má utilização pode corresponder de 30% a 40% de toda a produtividade de uma empresa.

**Date Created**

06/04/2004