

## RISCO ELETRÔNICO – FRAUDES NAS INSTITUIÇÕES DE ENSINO

Se a sua instituição ainda não sofreu nenhuma fraude, você deve estar se perguntando: Mas isto é possível?

A Sociedade Digital trouxe inúmeras vantagens, na esfera administrativa podemos citar como programas de gestão que permitem a integração de todas as informações da escola enquanto empresa e na esfera educacional, programas que possibilitam o apoio pedagógico. Mas a evolução não se limita a programas de software, abrange também ferramentas como a própria internet e conexões externas. Portanto, podemos falar desde softwares educacionais e administrativos até envio de acompanhamento por email e SMS.

Neste cenário é preciso entender que a evolução ocorreu não apenas para o bem, mas também no aspecto negativo, ou seja, as pessoas más intencionadas também evoluíram nas ferramentas que utilizam. Neste sentido, a tentativa de fraude cresce a cada dia e ferramentas como email são alvos fáceis para ludibriar uma pessoa.

Mas quais as consequências para uma instituição de ensino quando ela é vítima de fraude? E se a instituição tiver seu banco de dados invadido por intermédio de fraude e as informações de todos os seus alunos forem divulgadas?

Perceba que são inúmeras, desde uma imagem negativa que afeta na captação de novos alunos, como consequências jurídicas no caso acima.

E se o sistema for invadido e os alunos receberem mensagens de cobrança ou ainda pornográficas da instituição?

E por que alguém tentaria cometer uma fraude contra uma instituição de ensino?

Pode se dizer que por várias razões, entre elas simplesmente por prazer, quando se trata de *crackers* que desejam apenas mostrar poder, mas pode ser também com o objetivo de benefícios financeiros, ou ainda benefícios pedagógicos (quando se trata de notas). As situações são as mais diversas possíveis.

Diante do exposto, faça uma pausa para pensar, sua instituição já fez um levantamento dos riscos existentes? E das consequências se estes riscos vierem a se concretizar? Existem regras para uso do meio eletrônico? Há monitoramento?

---

Estamos todos preparados e cientes dos riscos e consequências? Estas informações são essenciais para uma gestão na Era da Informação e Tecnologia.

---

---

**Se não o fez, está na hora. Pensar nos tipos de fraudes, nas vulnerabilidades as quais a instituição está exposta, nas consequências e nas formas de prevenção.**

---

Pontos imprescindíveis: Tecnologia x pessoas, ou seja, recursos técnicos suficientes e conscientização de pessoas.

Termino este artigo com uma pergunta: Estamos todos preparados e cientes dos riscos e consequências? Estas informações são essenciais para uma gestão na Era da Informação e Tecnologia.

**Cristina Sleiman** é advogada e pedagoga, mestre em Sistemas Eletrônicos pela Escola Politécnica da USP e com extensão em Direito da Tecnologia pela FGV/RJ, extensão Educador Virtual pelo Senac São Paulo em parceria com Simon Fraser University. Sócia do escritório Cristina Sleiman Sociedade de Advogados, professora de Pós Graduação na Faculdade Impacta de Tecnologia, responsável pela coordenação de Prevenção de Crimes de alta tecnologia no ambiente corporativo na Comissão de Crimes de Alta Tecnologia da OAB/SP. Co-autora do audiolivro e livro Direito Digital no Dia a Dia publicado pela Saraiva. [www.cristinasleiman.com.br](http://www.cristinasleiman.com.br) / [cristina@sleiman.com.br](mailto:cristina@sleiman.com.br).

Humus – newsletter - 2011