PPP | PATRICIA PECK PINHEIRO ADVOGADOS

BOAS PRÁTICAS LEGAIS NO USO DA TECNOLOGIA DENTRO E FORA DA SALA DE AULA

Guia rápido para as instituições educacionais

2007

Apresentação

Os avanços da tecnologia e o advento da internet trouxeram impactos inimagináveis para a sociedade. Estamos diante de uma sociedade conectada, com e-mails, celulares, palms, chats, buscadores de informação, sites de notícia, comunidades online, sms, messenger, voip e outras ferramentas que até pouco tempo não faziam parte de nossa rotina diária de trabalho e lazer.

Neste novo cenário de mudanças tecnológicas nos deparamos com novos desafios e com novas formas de relacionamento que afetam o comportamento humano e consequentemente todos os aspectos que envolvem o desenvolvimento de uma sociedade, inclusive a **EDUCAÇÃO**.

Temos, enquanto educadores, o compromisso de orientar o educando para a vida, proporcionar situações que lhe permitam desenvolver habilidades e competências necessárias para ávida tarefa tanto profissional quanto de vida pessoal de um mundo cada vez mais plano, mais globalizado, sem barreiras espaciais e temporais, mas que os aspectos éticos e legais são colocados em questão em cada click.

Educar na sociedade digital não é apenas ensinar como usar os aparatos tecnológicos no ambiente escolar. Educar é preparar indivíduos adaptáveis e criativos com habilidades que lhe permitam lidar facilmente com a rapidez na fluência de informações, acompanhando as transformações e sendo parte delas, de modo responsável, ético e legal. É preparar cidadãos digitais para um novo mercado de trabalho que exige postura adequada, segurança da informação, respeito às leis, inclusive na Internet.

Neste sentido, para aplicar este princípio de educação atualizada e integrada com a realidade da Sociedade Digital atual, o professor deve antes de qualquer coisa entender que os jovens de hoje em dia são diferentes do que fomos quando na idade deles. Nascemos em uma era analógica bem diferente da era digital em que atenção múltipla é uma constante, em que o aluno exercita sua liberdade de expressão desde a mais tenra idade, pode viajar pelos países, conhecer a história e a geografia no click de um mouse.

É preciso que o educador esteja aberto para novos conceitos e novas formas de ensinar, é preciso também que esteja sempre atualizado e atento ao mundo deste novo aluno. Como apresentar o conceito de Direito Autoral, protegido por lei, de modo a orientar os projetos escolares e acadêmicos. Como deixar claro o respeito ao direito de imagem, a proibição constitucional do anonimato, e acima de tudo, que é “liberdade de expressão com responsabilidade”. Afinal, “diga-me com quem navegas, que te direi quem és”.

Índice

1.O Impacto da tecnologia na educação

1.1.Novos paradigmas, novas tendências e condutas

Conhecer os programas digitais que mais interessa seus alunos e descobrir o que motiva esse interesse é essencial neste novo cenário educacional. A melhor estratégia é buscar formas que possibilitem a utilização desses recursos e ferramentas de interesse dos alunos em benefício do aprendizado. A sala de aula não pode negar o impacto de um Google Earth em uma aula de História ou Geografia.

Repare que o perfil do estudante mudou muito, hoje ele sai da escola, vai para casa e faz tudo ao mesmo tempo: assiste televisão, navega na Internet e faz a tarefa, sem contar que muitas vezes faz varias atividades ao mesmo tempo, e ainda em modo colaborativo, se relacionando com seus colegas e amigos pelos comunicadores instantâneos. Está claro que novas habilidades foram desenvolvidas. Temos que buscar atividades interessantes para conquistar o interesse e a atenção deste aluno. É um desafio e tanto, mas temos que encarar de forma positiva, pois o contato com o mundo em que o jovem vive atualmente pode ser um grande aliado no processo ensino aprendizagem, mas vai depender da criatividade e dedicação do professor. O tempo não volta e a tecnologia veio para ficar, não há como negar este fato.

Como toda novidade, a Internet (para citar apenas um dos meios digitais atuais) ainda é usada sem limitações, o que nos traz uma grande preocupação. É certo que se trata de uma ferramenta que proporciona maravilhas além de auxiliar e potencializar a disseminação do conhecimento, mas devemos estar atentos, precavidos, orientando nossos alunos em como se protegerem das ameaças eletrônicas.

O que a experiência nos mostra é que as pessoas querem experimentar de tudo e acabam ultrapassando limites éticos e legais. Mesmo no ambiente virtual, a ninguém cabe alegar desconhecimento das leis, e as mesmas se aplicam, ao contrário do que muitos imaginam. Portanto existe uma necessidade de se orientar o jovem para uso correto da rede, da tecnologia de um modo geral, indicando as conseqüências de seu mau uso.

Nosso grande desafio é como inserir e trabalhar com os novos meios digitais de forma a favorecer o processo ensino aprendizagem, não só agindo e utilizando de forma ética e legal, mas também educando nossos alunos para o uso correto de tais recursos, pois, precisamos protegê-los, prepará-los e educá-los diante dos novos parâmetros dos quais nos deparamos.

1.2.Os novos riscos trazidos pela tecnologia

Jovens e adultos precisam aprender sobre a responsabilidade de seus atos na Sociedade Digital, em que as relações são cada vez mais eletrônicas e as testemunhas são máquinas. Cada um é responsável não somente pelo que escreve, mas também pelo que “assina”, ou seja, com apenas um clique se está assinando um contrato, concordando com os termos de navegação daquele determinado *website*, se está passando para frente um boato por e-mail, fazendo download de uma imagem, praticando pirataria.

Quais são os problemas que mais atingem as pessoas?

- Plágio;
- Pirataria;
- Más amizades virtuais;
- Assédio digital;
- Falta de boas maneiras online;
- Limites da liberdade de expressão;
- Uso de imagens – Privacidade;
- Segurança – fraude eletrônica, vírus.

Este novo cenário exige uma postura reflexiva e flexível, precisamos educar para o hábito da leitura de políticas de segurança, privacidade, termos de uso e de serviço e reserva de direitos autorais. É preciso pensar várias vezes antes de publicar algo *online* porque os resultados de um conteúdo mal

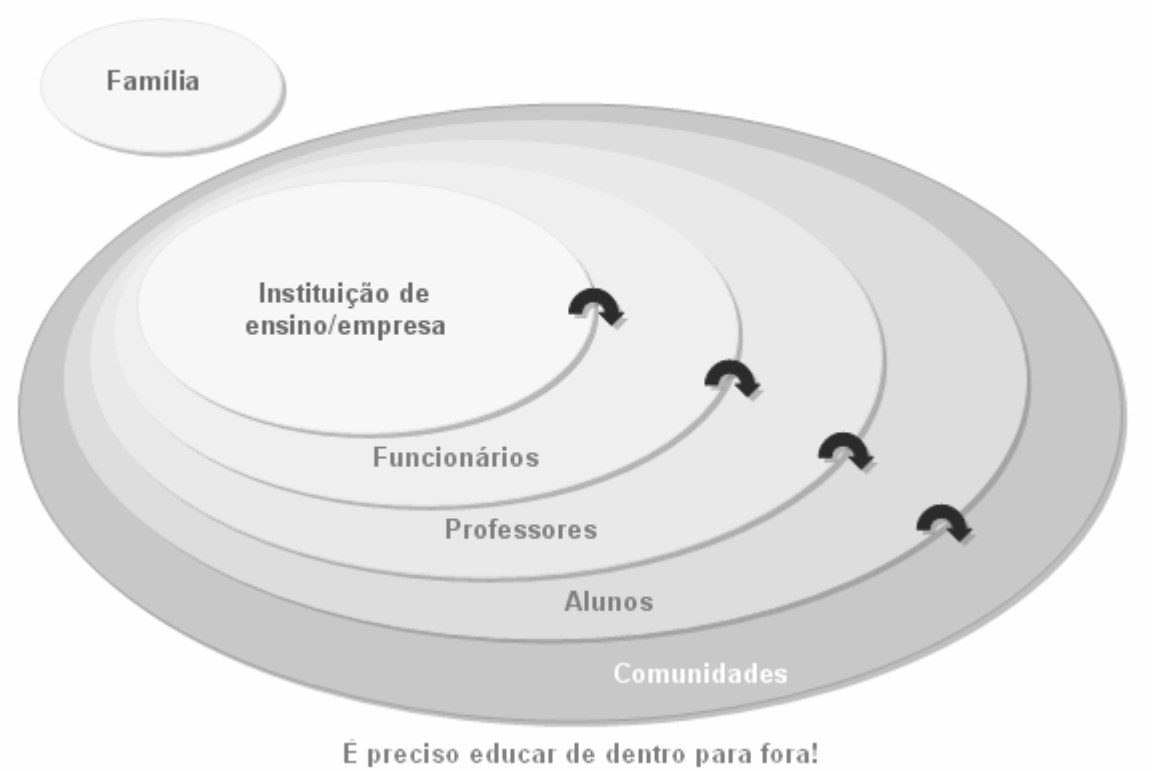
colocado podem ser avassaladores e podem persegui-lo tempos depois. O usuário pode ser punido tanto no âmbito escolar quanto no judiciário.

Os jovens precisam de ajuda para desenvolver habilidades que lhe permitam reconhecer os perigos *online* através de uma orientação adequada para que possam desenvolvê-la e aplicá-la por si. É inevitável, por exemplo, que usuários se depararem com pornografia na Internet, *sites* que promovem a delinqüência (destruir, construir armas, falsificar documentos, etc), *sites* de jogos, entre outros. **Sua decisão neste momento fará toda a diferença. O poder está na mão do usuário.**

Quais são os problemas que mais atingem as Instituições?

- Uso indevido de senha;
- Vazamento Informação Confidencial;
- Furto de Dados e Concorrência Desleal;
- Uso não autorizado da Marca na Internet (ex: Orkut);
- Responsabilidade civil por mau uso da ferramenta de trabalho tecnológica por funcionário (uso email corporativo para fim pessoal);
- Pirataria, download de softwares não homologados, baixa de músicas, imagens, contaminação por virus e trojans;
- Problemas com contratos de TI – Terceirização;
- Segurança – fraude eletrônica, virus e Privacidade (Monitoramento).

Tanto os professores, como os pais de alunos, também devem ser educados para que aprendam como proteger e educar aos jovens. É preciso que as instituições educacionais promovam ações que os deixem informados sobre tecnologia, e acima de tudo preparados para lidar com esses problemas quando surgirem. A melhor forma de atingirmos este objetivo é pensar numa educação de dentro para fora:



É preciso educar de dentro para fora!

Ainda em meio ao bombardeio de informações, é necessário instruir os usuários a distinguirem fatos de opiniões na Internet. Devem ser elaborados exercícios sobre observação e decisão quanto a conteúdo de *sites*, com uma visão crítica, inclusive sobre a veracidade dos mesmos.

É preciso conscientizar os jovens de que as boas maneiras existem, não estão fora de moda e se aplicam na comunidade virtual seja qual for a situação. As instituições educacionais, junto com os professores são responsáveis por criar uma cultura de uso responsável contribuindo para uma sociedade mais digna, mais ética.

Deparamos-nos desta forma com a necessidade de repensarmos os modelos educacionais para que possam abranger tais questões que refletem um compromisso com o exercício da **Cidadania Digital.** A atualização do modelo educacional e de negócio das instituições de ensino é essencial. O novo desafio é educar sob os novos parâmetros desta realidade globalizada e conectada em tempo real.

É preciso estar atento, pois temos que utilizar e incentivar o uso correto das tecnologias, lembrando que a instituição é responsável pelas ferramentas de trabalho tecnológicas que disponibiliza para alunos e funcionários, bem como pelo uso que fazem delas e que qualquer incidente alcança a instituição enquanto pessoa jurídica na esfera civil, seus administradores e até mesmo professores e alunos (pessoa física) na esfera criminal.

Portanto é necessário que tomemos algumas precauções para trazer uma maior proteção jurídica para a instituição, a marca, aos mantenedores, gestores, funcionários, fornecedores, parceiros, alunos, pais e comunidade.

A gestão do risco eletrônico é um exercício diário que envolve não só recursos técnicos, mas também a responsabilidade do educador e também do empregador da era digital em educar os usuários sejam funcionários ou alunos com os novos valores éticos e legais da mesma. Há novas posturas de trabalho, quando deixamos de ser presenciais, quando estamos acessíveis e acessando de todo o lugar, com a mobilidade, a banda larga e a convergência.

Este guia tem como principal objetivo orientar o professor, o coordenador e o gestor das instituições educacionais nas boas práticas de Direito Digital que irão auxiliar aos educadores a levarem estas questões a seus educandos a fim de promover a proteção do usuário enquanto indivíduo e reduzir os riscos da tecnologia no uso de ambientes eletrônicos em seu negócio, além de proteger os principais ativos que são cada vez mais intangíveis, como Marcas, Know-How, Direitos Autorais, Patentes, Software, Bancos de Dados de forma que possam posteriormente levar seus conhecimentos também à sala de aula e dar início a um trabalho de orientação a seu aluno.

1.3.O professor e a tecnologia

O professor tem um papel muito importante neste novo cenário. Além de ser muitas vezes um modelo para seu aluno, o professor tem um contato direto na formação do mesmo. Portanto tem uma responsabilidade que se compara com poucos. Mas é importante que tenha consciência da necessidade de sua adequação a esta nova realidade, para que possa aumentar a sua proximidade com os educandos.

Utilizar ou não os meios tecnológicos como apoio pedagógico, não é mais passível de discussão, mas a sua forma de utilização com certeza sempre o será. O professor precisa se atualizar, sob pena de ser atropelado pelo tempo e pelas novas tecnologias, que, na verdade, jamais superarão o mestre, a relação professor-aluno, gerando então um verdadeiro vazio, um precipício que já estamos vivenciando na falta de referências e valores dos jovens online.

Mas o que o professor tem a ver com as questões legais da tecnologia? A questão legal tem a ver com qualquer cidadão que faça uso das tecnologias, não apenas do professor do aluno ou do gestor, mas sim do individuo enquanto membro da sociedade. Mas o professor, não pode esquecer de seu compromisso com a educação. Portanto tem o dever de estar atento à nossa legislação e orientar a seus alunos para que percorram o caminho certo nesta jornada, tirando uma dúvida em sala de aula sobre infração de direito autoral, sobre uso de imagem, sobre privacidade, sobre spam, sobre o limite entre a brincadeira, a piada e a difamação em dimensão global, pois é isso que a Internet representa.

O que o professor pode fazer? O professor pode e deve estar atento às novidades tecnológicas bem como aos riscos e novos meios de fraude e atos ilícitos. Desta forma terá conhecimento suficiente para abordar tais questões em sala de aula.

Veja abaixo algumas dicas:

- Leve a questão à direção da instituição;
- Pense em estratégias que abordem as questões legais dentro de conteúdos já programados;
- Explique para seus alunos o que são direitos autorais;
- Ensine-os a fazer uso de referência em suas situações;
- Mostre a Lei de Direitos autorais;
- Mostre o Código Penal e a existência de alguma tipificações como o crime de infração de direito autoral, e outros, comuns como calúnia, injúria e difamação.

1.4.A instituição de ensino e a tecnologia

As tecnologias trazem um mar de possibilidades para utilização no âmbito educacional, entre eles um melhor aproveitamento pedagógico, de forma a potencializar o processo de ensino aprendizagem. Podemos encontrar muitas propostas de metodologias, ferramentas e atividades a serem desenvolvidas pelos alunos na rede interna das instituições e também na internet. Realmente enquanto educadores não podemos ficar parados diante de tantas oportunidades que nos afrontam. Não só devemos, mas temos o dever de aproveitá-las da melhor forma, o dever de buscar novos pensamentos e de estarmos sempre atualizados.

Não há o que se falar em educação se não conseguirmos estar inseridos na realidade de nossos educandos. Precisamos acima de tudo estar preparados para este desafio, buscando desenvolver as habilidades necessárias, bem como conhecer os recursos disponíveis e suas possibilidades.

Toda esta revolução afeta diretamente a forma de relacionamento humano. Temos alguns recursos como chats, fóruns, comunidades entre outros que estão disponíveis a todos e muitos com acesso livre. A grande questão está no comportamento do ser humano diante desta nova forma de se relacionar. Temos visto uma tendência ao anonimato, no entanto, a Constituição Federal em seu art. 5º. proíbe expressamente tal conduta. É comum os usuários pensarem que estão escondidos por traz de um monitor e por este motivo acabam por optar pela prática de condutas ilícitas ou ainda a praticam por pura ignorância de nossas leis.

A sociedade digital se apresenta de forma ativa e permite uma comunicação dinâmica. Não podemos nos ausentar desta discussão. É preciso trabalhar os novos paradigmas de forma ética e dentro dos conceitos legais através de uma educação focada não apenas no conteúdo tradicional, mas no **"conteúdo necessário à vida em sociedade digital".**

Temos que considerar que as ferramentas tecnológicas se utilizadas para o fim ilícito podem causar grandes danos e provocar conseqüências por toda sua vida.

Assim como o professor a instituição educacional deve ficar atenta a seu compromisso, proporcionando a seus corpo docente e discente a possibilidade de aprendizado atualizado e continuado. Cabe ao gestor criar uma estratégia de comunicação pedagógica para levar à sua instituição e à sua comunidade este papel de responsabilidade social, para a prevenção e a educação no uso correto dos meios eletrônicos.

É preciso educar para utilizar. Criar uma cultura de uso ético e legal, de forma que a instituição estará não apenas cumprindo com seu papel educacional e social, mas também se protegendo e contribuindo para a evolução da sociedade.

Portanto cabe à instituição promover não apenas a inclusão digital, mas sim a "Educação Digital", pois a simples entrega da tecnologia sem o devido preparo e orientação pode causar danos irreparáveis.

► É importante capacitar não apenas os professores para que possam levar estas questões à sala de aula, mas também capacitar e conscientizar todos os funcionários da instituição! ◄

1.5.Os pais e a tecnologia

Os pais devem estar atentos aos passos de seus filhos, sendo responsáveis legais por estes, por ação e por omissão, por culpa na vigília, por mais analógico que sejam.

É muito comum escutarmos de pais que não querem invadir a privacidade dos filhos. Mas precisamos distinguir orientação com invasão. É preciso que os pais acompanhem a vida de seus filhos e se preocupem com sua identidade digital, bem como suas ações no campo virtual, pois os efeitos serão sempre bem reais. **Lembre-se embora tenha sido criado na era analógica, isto não o eximirá de responsabilidade por não saber o que seu filho estava fazendo no computador!**

O que os pais podem fazer? Os pais devem acompanhar o avanço tecnológico com atenção especial aos riscos existentes, procurando, por exemplo, saber o que é um Orkut e como ele funciona, buscando notícias, compartilhando estas informações com seus filhos. Ler os Termos de Uso dos Serviços Online é essencial, até para apontar para os filhos o que há em seu conteúdo, já que muitas vezes estes dão OK sem ler, sem saber o que estão assumindo, se obrigando. **É fundamental saber quais comunidades seu filho está associado e qual sua participação dentro dela.**

Além disso, os pais devem deixar claro para seus filhos o que é crime eletrônico e suas conseqüências, ou seja, o que na rede pode ser considerado como crime. Esta abordagem deve buscar gerar uma reflexão sobre o que é certo e o que é errado. O que é perigoso, o que é uma simples brincadeira e o que pode virar ação judicial.

A tecnologia que aproxima também é a que distância. Assim como tem muitos pais e filhos que hoje conseguem se relacionar melhor, falando por e-mail, também há aqueles que não conversam nunca, pois o filho está sempre falando com amigos no comunicador instantâneo, nas comunidades, e não se interessa mais nas conversas de família a mesa, na hora das refeições, que é como se fazia antigamente. Se estes pais não puderem fazer parte dos amigos virtuais do filho, dos favoritos, então eles estão excluídos.

O diálogo é a peça-chave no quebra-cabeça da era da informação. Os pais devem ser uma fonte de informação para seus filhos digitais, e não apenas o Google (exemplo de buscador da internet). Por isso, este tema deve também ser debatido com a escola, com os professores e com a direção. Uma atuação integrada com certeza contribuirá para uma sociedade muito melhor.

2.Utilizando as tecnologias dentro da sala de aula

2.1.Aplicações

Existem várias formas de se utilizar as tecnologias a seu favor em sala de aula. Entre elas podemos encontrar WebQuest uma atividade que promove a pesquisa não só online, mas também impressa. Existe também atividades como WebGincanas, ferramentas como blogs, comunidades e fóruns que promovem o desenvolvimento e criatividade do educando. O próprio uso já de e-learning, de quadro interativo, de sala virtual para fazer dever de casa ou ter reposição de matéria, bem como diversos softwares que dão mais vida para o conteúdo escolar, como os relacionados à biologia e ciências, ou o próprio serviço do Google Earth, que pode apoiar uma aula de Geografia.

Mas como trabalhar os aspectos éticos e legais sem podar o desenvolvimento educacional? A resposta é muito simples, devemos encarar como um conjunto a ser utilizado dentro e fora da sala de aula. Se disponibilizarmos as tecnologias sem um amparo educacional, com certeza os alunos irão encontrar uma utilidade para elas, mas seu uso incondicional e sem limites pode ser desastroso para a sociedade.

Pense numa comunidade sem leis, onde todos pudessem fazer o que querem, sem restrições ou penalidades. Seria um caos, uma briga, porque infelizmente estaríamos voltando para o estado de natureza, a lei do mais forte. A sociedade precisa de regras para garantir equilíbrio entre os indivíduos e as organizações.

O mesmo ocorre com o espaço virtual, é preciso regras para um convívio digital saudável. A questão é que algumas delas já existem, pois nossa legislação é perfeitamente aplicável, pois não se trata de um mundo paralelo, mas sim uma extensão de nossos atos e condutas que podem sim ser punidos. O mundo virtual reflete o real, e vice-versa!

2.2.Blogs e comunidades

Os WebLogs ou blogs, eram utilizado originalmente em navios ou aviões para relato de informações importantes. Hoje conhecidos como diário online por se encontrarem num espaço virtual, possuem diversas funções e podem ser utilizados para ajudar no desenvolvimento de diversas áreas do conhecimento. No início foram criados blogs individuais e para relatos pessoais. Com o tempo foram aparecendo blogs comunitários e com assuntos mais diversos possíveis. Hoje temos blogs até mesmo de jornalista relatando acontecimentos do mundo todo.

As comunidades trazem uma forma de convívio online, seja de forma assíncrona ou síncrona. Geralmente oferecem recursos de fóruns, chats e agrupamentos por interesse. Tornou-se muito comum a utilização de comunidades de prática, onde as pessoas se reúnem por interesse e compartilham as informações de forma contínua.

Ambos podem trazer muita contribuição para o relacionamento de uma turma de alunos, principalmente para produção colaborativa e incentivo a pesquisa e atividades fora da sala de aula. No entanto, precisam ser ensinados alguns limites.

► Aprendizagem de forma divertida e desprendida é uma forte aliada! ◄

2.3.Pesquisas online

A Internet foi concebida como um ambiente de informação e pesquisa, depois evoluiu para um ambiente de transação e relacionamento. Por isso, de certo modo ela dá uma dimensão do conhecimento humano atual, sejam coisas importantes, notícias, ou banalidades, cotidiano, vida das pessoas comuns. Há espaço para tudo e todos. Isso é de grande valia para a educação. É possível fazer uma pesquisa em tempo recorde e com eficiência. No entanto a internet por possibilitar o acesso a todos, não garante a veracidade das informações. Muitas pessoas publicam suas opiniões

como sendo a verdade absoluta e não como um tópico de discussão. Alem daquelas que editam, distorcem, mentem. Não se pode acreditar em tudo, só porque está na Internet.

Logo, apesar de podermos encontrar na rede uma grande quantidade de conteúdos desenvolvidos por sistemas colaborativos, onde todos os usuários podem contribuir, é preciso que fiquemos atentos para não sermos enganados por informações falsas. **Ensinar esta capacidade crítica, de separar o que é bom do que não tem valor, é papel do Educador!**

2.4.Riscos

A tecnologia pode ser utilizada para o bem, ou para o mal. Ela pode facilitar a comunicação entre as pessoas, como um e-mail pode ser o melhor canal de dialogo para um assunto difícil entre um pai e um filho, ou ao contrário, o uso maciço do messenger, por exemplo, pode excluir o pai do relacionamento e convívio social com seu filho. Tudo depende de como fazemos uso dela, de como educamos.

Qual o risco que apresentam os blogs e comunidades quando utilizados em sala de aula? A internet é um poderoso meio de comunicação, mas temos que ter em mente que no espaço virtual tudo prova. Portanto, ao publicar uma opinião não podemos confundir liberdade de expressão com irresponsabilidade, ao contrário, a Constituição Federal de 1988, juntamente com o Código Civil e o Código Penal, todos em vigor, determinam **"liberdade com responsabilidade de expressão".**

Nosso direito vai até onde começa o direito do próximo. Ofender alguém além de não ser liberdade de expressão é crime tipificado no Código Penal brasileiro, podendo ser caso de injuria, difamação e/ou calúnia. **Portanto, temos que ficar atentos ao que expressamos pela internet. Estamos colocando por escrito e assinando embaixo!**

É comum a utilização de blogs, por exemplo, por professores para relatar suas atividades com cada turma, registrando acontecimentos, encontros e até mesmo fotos, no entanto é preciso ter uma autorização dos alunos ou ainda dos pais de alunos quando estes forem menores de idade, para que possa ter suas fotos publicadas na internet ou em qualquer outra mídia.

O mesmo vale para os alunos que ao publicarem fotos em seus blogs a rigor precisariam ter uma autorização das pessoas fotografadas, sem contar com a questão de direitos autorais do autor da foto ou pintura escaneada.

Apesar de parecer engraçado criar uma comunidade para falar mal de um professor, a mesma pode gerar grandes conseqüências legais para o Aluno, seus Pais e a própria Instituição de Ensino. É preciso ter cuidado, orientar no uso correto, monitorar, gerar advertências, retirar do ar o conteúdo inadequado que estiver associado com o nome da Instituição. Não podemos ficar de braços cruzados.

► A melhor medida de prevenção é a informação e a educação! ◄

2.5.Boas práticas – identidade digital do aluno

Um dos maiores males no ambiente virtual é o anonimato, no sentido de favorecer a prática de ilícitos, de atividades antiéticas e até crimes. Por isso, dentro do ambiente escolar, é fundamental que haja a identificação individual e única do Aluno quando o mesmo estiver fazendo uso de ambientes eletrônicos. Seja o computador dentro da sala de aula, no laboratório, na biblioteca.

Cabe a Instituição conferir uma Identidade Digital para o Aluno, de modo a que se ocorrer algum incidente, será possível verificar sua autoria. Isso serve como medida de prevenção, para coibir a conduta, já que sendo pego saberão quem foi, assim como garante uma medida de reação, aonde ocorrendo a conduta é possível achar o infrator, e assim adverti-lo, orientá-lo, ou se for o caso, praticar algum tipo de penalidade, como suspensão do uso do ambiente eletrônico por um período, ou em casos mais graves, até a expulsão.

Muitos ambientes educacionais não fazem este tipo de controle mínimo, que garante o bem estar social digital. E isso envolve inclusive aumentar a responsabilidade civil por danos causados a terceiros, uma vez que tudo vai ficar registrado como tendo sido feito pelas "maquinas em nome da

Instituição", então gera nexo causal e responsabiliza a mesma, que fica incapacitada de saber de fato quem foi, por não ter um modelo adequado de Identidade Digital.

Além disso, como orientar seu Aluno? Comece com atividades que já possuem um sistemas ou metodologia estabelecida, como WebQueste ou WebGincana, que já trazem consigo uma orientação de sites a serem utilizados nas pesquisas. Procure informar a seu aluno que é necessário buscar sites confiáveis e quando não houver essa certeza, devemos procurar comparar a pesquisa em diversas fontes.

Apresente artigos de jornal sobre situações de risco na Internet, com exemplos de casos, o que aconteceu, como poderia ter sido evitado, qual foi a penalidade dos envolvidos, quais leis se aplicam. Este tipo de orientação ajuda inclusive a evitar que os alunos sejam vítimas na Internet, especialmente de situações de assédio digital, pedofilia, exposição de imagem, receptação de conteúdo pirata ou ilegal, fraude com cartão de crédito, fraude em Internet Banking, ser enganado por uma loja virtual, ser contaminado por vírus achando que tinha recebido um cartão de amor, entre outros exemplos.

Há ainda a necessidade de orientar no tocante ao uso do celular, que se tornou uma febre dentro das Instituições Educacionais, mas há momentos em que precisa estar desligado, e isso não vale apenas para o cinema ou o teatro, vale para dentro da sala de aula também!

► Procure por formas de pesquisa que direcionem seus alunos para sites seguros! ◄

■ ■ ■

3.Utilizando as tecnologias fora da sala de aula

3.1.Aplicações

Esta é uma questão mais delicada, porque alguns educadores cometem o equívoco de pensar que a conduta de seus alunos fora da escola não afeta seu trabalho ou ainda a própria escola.

Lembre-se que se o aluno se envolve em alguma atividade ilícita ou uma briga, por exemplo, e este estiver com o uniforme da escola, a mesma poderá ser atingida. Assim também com o ambiente virtual, o que os professores e alunos fazem em nome da escola podem alcançar a mesma.

Além da questão de responsabilidade civil, a Instituição e seus educadores devem se preocupar com sua responsabilidade social e compromisso com a educação para uma sociedade melhor, para o exercício da cidadania.

Primeiramente, a mais comum é o e-mail, utilizado muitas vezes como uma extensão da instituição, seja para o contato entre professor e aluno ou terceiros. O que os professores dizem nos emails correspondem à opinião da Instituição. Por isso, é fundamental orientar sobre uso ético e legal desta ferramenta tão útil que já faz parte de nossas vidas. Há ainda os blogs, as comunidades, o uso dos comunicadores instantâneos, sem falar no celular, no acesso a cybercafés e lanhouses.

► Crie espaço em sala de aula que envolva discussões e exemplos reais que acontecem no dia a dia fora da escola! ◄

3.2.Riscos – principais infrações dos usuários de tecnologia

Quando o e-mail é disponibilizado para os alunos, a instituição também é responsável por orientar para seu correto uso. Pois é como uma extensão das instalações da instituição. Enquanto o aluno navega ou faz uso do espaço virtual da instituição, está sob sua responsabilidade.

No tocante aos Blogs, temos que orientar os alunos para que não façam uso dos mesmos de forma irresponsável. Por exemplo, a questão de direitos autorais, vale tanto para dentro da instituição, como também quando o aluno está se relacionando do lado de fora dos muros da escola.

O mesmo se aplica para as comunidades. O que o aluno ou professor faz numa comunidade em nome da instituição pode gerar responsabilidade civil para a mesma que tem, no entanto direito de regresso contra a pessoa física que provocou o dano. **Você já fez uma pesquisa para saber quais são as comunidades, blogs, fotologs que estão montadas com o nome da sua Instituição ou fazendo menção a ela ou a seus dirigentes e professores?**

Outra preocupação é orientar os alunos para que não cometam infrações penais no intuito de brincadeira, assim como o caso recente do rapaz que pediu ajuda para se matar num forum. Todos os envolvidos, que deixaram uma mensagem aconselhando ou ensinando como fazer, podem e devem ser indiciados, por crime de instigo ao suicídio.

► Tudo que estiver escrito em uma mensagem "@nomeinstituição.com.br ou @nomeinstituição.edu.br responsabiliza a mesma. ◄

3.3.Boas práticas – educação do usuário digitalmente correto

Em diversos trabalhos que realizamos com Instituições de Ensino vimos que com um pouco de informação e orientação, a maior parte dos alunos acata as regras e deixa de cometer as condutas indevidas, por uma questão de passar a saber com mais clareza o limite entre "certo e errado". Isso é feito de diversas formas:

- Palestras de Conscientização com convidado especialista em Direito Digital (que pode ser advogado, delegado, perito, procurador, promotor, juiz);
- Aula de Cidadania e Ética Digital dentro da programação escolar;
- Cartilha sobre Uso Ético e Legal da Tecnologia;
- Reunião com pais específica sobre o tema;
- Inserção de cláusulas específicas sobre o assunto no contrato de matrícula;
- Revisão e atualização do Código de Ética do Aluno para tratar destes temas;
- Revisão dos contratos de trabalho dos funcionários para tratar destes temas;
- Elaboração e implementação de Política de Segurança da Informação e outras normas;

A ninguém cabe alegar desconhecimento da lei

Art. 21 CP "O desconhecimento da Lei é inescusável"

Cabe citar que o Código Penal Brasileiro não imputa a tipificação apenas no caso de crime doloso, mas também para o crime culposo, cuja o agente não tinha intenção de cometê-lo. A única forma inescusável seria a falta de capacidade do agente para entender a ilicitude do fato ou se não pudesse exigir conduta diversa. E quando o infrator é menor de idade, quem responde são os pais!

4.Responsabilidade digital da instituição educacional

4.1.Quais são os problemas?

Para este trabalho a palavra responsabilidade tem o significado específico de "ter que responder por um ato danoso". Portanto responsabilidade digital da instituição educacional é sua obrigação de reparar os danos causados a terceiros através de utilização dos meios digitais, tenham sido praticados por funcionários, alunos, seja em seu nome ou não. Cabe ainda ressaltar que tal responsabilidade independe de culpa ou dolo.

Cumpre destacar que de acordo com o Novo Código Civil, a responsabilidade civil foi ampliada influenciando diretamente nas questões jurídicas relacionadas aos meios digitais.

É comum empregados e/ou professores utilizarem de e-mail corporativo, por exemplo, para questões pessoais. O problema é que esse e-mail pode ser interpretado como opinião da empresa, causando danos irreparáveis. Outro exemplo comum, é comunidades que utilizam a logomarca da instituição para fazer comentários desagradáveis que podem afetar a imagem da empresa.

Comunidades, Chats, Fóruns e Blogs, são utilizados por alunos para denegrir a imagem da instituição ou dos professores. A falta de procedimento para identificação do usuário também deve ser encarado como uma preocupação, pois a identidade digital é necessária, até mesmo para identificação de autoria. Se é detectado um crime cometido por intermédio de ferramentas digitais e constata-se que o endereço IP do autor vem de sua instituição você deve estar apto a identificar quem era o usuário logado naquele momento.

A questão da responsabilidade

O Código Civil (Lei nº 10.406/02) trata das relações entre as pessoas, estabelecendo responsabilidades, inclusive no ambiente de trabalho. Verifique o texto dos artigos abaixo:

Artigo 186 - Aquele que, por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem, ainda que exclusivamente moral, comete ato ilícito.

Artigo 1016 - Os administradores (cargo de gerente para cima) respondem solidariamente perante a sociedade e os terceiros prejudicados, por culpa no desempenho de suas funções.

4.2.O que pode ser feito?

Uma das questões mais relevantes é gestão de interface tanto com os alunos como com os funcionários, onde se deve estabelecer os limites éticos, de privacidade, segurança e produtividade na aplicação da mesma dentro da instituição. Toda a forma de controle deve estar acordada entre as partes de modo transparente e inequívoco.

Para evitar riscos é fundamental a empresa ter um conjunto de Políticas Corporativas que trate destes temas, sendo requisito a Política de uso de E-mail, Internet e TI por funcionários, bem como um **Código de Conduta** para os alunos. A Política de Segurança da Informação deve incluir a questão do Monitoramento e da Privacidade, a Política de Compartilhamento de Conteúdo, a Política de Documentação Eletrônica, a Política de uso Ético de E-mail Marketing, entre outras. Todos estes termos precisam retratar a filosofia da instituição, devendo trazer claramente os comportamentos vedados e suas respectivas penas. É preciso usar a própria tecnologia para induzir comportamento. A regra legal deve ser traduzida em linguagem de software e fazer parte da navegação, e-mail e acesso a Internet.

Todo indivíduo é responsável por seus atos, assim acontece também no mundo virtual. Cada usuário é responsável por sua conduta. Embora a instituição tenha responsabilidade civil pelo que é feito em suas dependências, quando tiver que ressarcir algum dano poderá cobrar este da pessoa física que o causou.

Sendo este menor de idade, seus pais serão responsabilizados, ou aquele que tem sua guarda. O menor de 18 de anos é protegido pelo Estatuto da Criança e do Adolescente ECA – Lei 008.069-1990, cuja em seu art. 103, considera como ato infracional as condutas descritas como crimes ou contravenção no Código Penal. Segundo art. 101 do ECA, a autoridade responsável poderá tomar as medidas como de inclusão em programa comunitário ou oficial.

Não podemos esquecer que o Código Civil também abrange esta questão e responsabiliza os pais quando filhos menores cometem certos atos considerados ilícitos, entende-se que os pais têm obrigação de dirigir a educação e exercer uma espécie de poder de vigilância sobre seus filhos menores. Quando estes causam danos a outrem entende-se que faltou com seu dever de vigilância, sendo necessário provar que não houve descuido e não foi negligente.

TABELA DE INFRAÇÕES DIGITAIS MAIS FREQUENTES NA VIDA COMUM DOS USUÁRIOS		
Falar em um chat, blog ou comunidade que alguém deve se matar ou sugerir como fazê-lo.	Instigação ou auxílio ao suicídio	Art. 122 C.P.
Falar em um chat que alguém cometeu algum crime (ex. ele é um ladrão...)	Calúnia	Art.138 do C.P.
Dar forward para várias pessoas de um boato eletrônico	Difamação	Art.139 do C.P.
Enviar um e-mail para a Pessoa dizendo sobre características dela (gorda, feia, vaca,...)	Injúria	Art.140 do C.P.
Enviar um e-mail dizendo que vai pegar a pessoa	Ameaça	Art.147 do C.P.
Enviar um e-mail para terceiros com informação considerada confidencial	Divulgação de segredo	Art.153 do C.P.
Fazer um saque eletrônico no internet banking com os dados de conta do cliente	Furto	Art.155 do C.P.
Enviar um vírus que destrua equipamento ou conteúdos	Dano	Art.163 do C.P.
Copiar um conteúdo e não mencionar a fonte, baixar MP3 que não tenha controle como o WMF	Violação ao direito autoral	Art.184 do C.P.
Criar uma Comunidade Online que fale sobre pessoas e religiões	Escárnio por motivo de religião	Art.208 do C.P.
Colocar foto em Comunidade Online com gestos obscenos	Ato obsceno	Art.233 do C.P.
Criar uma Comunidade dizendo "quando eu era criança, eu roubei a loja tal…"	Incitação ao Crime	Art.286 do C.P.
Criar uma Comunidade para ensinar como fazer "um gato"	Apologia de crime ou criminoso	Art.287 do C.P.
Enviar e-mail com remetente falso (caso comum de spam) ou Fazer cadastro com nome falso em uma loja virtual.	Falsa identidade	Art.307 do C.P.
Entrar na rede da empresa ou de concorrente e mudar informações (mesmo que com uso de um software)	Adulterar dados em sistema de informações	Art.313-B do C.P.
Se você recebeu um spam e resolve devolver com um vírus, ou com mais spam	Exercício arbitrário das próprias razões	Art.345 do C.P.
Participar do Cassino Online	Jogo de azar	Art.50 da L.C.P.
Falar em um Chat que alguém é isso ou aquilo por sua cor	Preconceito ou Discriminação de Raça, Cor, Etnia, Etc.	Art.20 da Lei 7.716/89
Ver ou enviar fotos de crianças nuas online (cuidado com as fotos de seus filhos e dos filhos de seus amigos na net)	Pedofilia	Art.247 da Lei 8.069/90 "ECA"
Usar logomarca de empresa em um link na página da internet, em uma comunidade, em um material, sem autorização do titular, no todo ou em parte, ou imitá-la de modo que possa induzir a confusão.	Crime contra a propriedade industrial	Art.195 da Lei 9.279/96
Empregar meio fraudulento, para desviar, em proveito próprio ou alheio, clientela de outrem, por exemplo, uso da marca do concorrente como palavra-chave ou link patrocinado em buscador.	Crime de Concorrência Desleal	Art.195 da Lei 9.279/96
Monitoramento não avisado previamente, coleta de informações espelhadas, uso de spoofing page	Interceptação de comunicações de informática	Art.10 da Lei 9.296/96
Usar copia de software sem ter a licença para tanto	Crimes Contra Propriedade Intelectual Pirataria"	Art.12 da Lei 9.609/98

5.Protegendo a instituição de ensino – gestão do risco eletrônico

5.1.Como levar a questão do uso ético e legal para os alunos?

O primeiro passo é repensar a proposta pedagógica para que contemple a utilização de estratégias e abordagens específicas ligadas ao cotidiano de seus alunos. Uma proposta que incentive a permanente atualização dos docentes e sua capacidade criativa de trabalhar situações reais do cotidiano dos alunos.

Mesmo que isto não aconteça como primeira ação, é possível trabalhar nos planos de aula, mas lembre-se sempre com aprovação da direção da Instituição.

Neste novo modelo de sociedade é necessário que a educação acompanhe não só a revolução do conhecimento, mas também os novos parâmetros de convívio social. As instituições educacionais, enquanto compromissadas com o futuro de seus alunos devem se preocupar com sua educação enquanto **"cidadão digital"**. Devem buscar formas de ensino aprendizagem que desenvolva em seus educandos conhecimentos e habilidades necessárias para este novo cenário e seja capaz de se proteger contra os perigos da rede, bem como saibam agir de forma ética e legal para que não se tornem infratores ao acaso.

Existe ainda o problema de acesso a sites que não deveriam ser liberados aos alunos e neste caso a escola pode ser responsabilizada pelo acesso em suas dependências (sites de conteúdo pornográfico, jogos de azar, entre outros). Assim, se um aluno menor de idade acessa um site de pedofilia dentro de sua instituição, por intermédio de uma ferramenta disponibilizada em laboratório ou biblioteca, fica a instituição responsável pela utilização dos mesmos bem como pela segurança de seus alunos.

O que pode ser feito? As instituições educacionais podem e devem dedicar em seu planejamento e grade curricular algumas horas para educação digital, ou seja, para educar quanto ao uso ético e legal dos meios digitais. Tais horas podem ser inseridas numa disciplina já existentes ou ainda numa grade extracurricular. Aconselha-se ainda a elaboração de material didático específico para o tema, além de aulas com professores capacitados.

É preciso além de uma ação educacional, monitorar a utilização das ferramentas disponibilizadas pela instituição para seus alunos, bem como implementar um sistema de bloqueio à sites indevidos e distribuição de uma cartilha com dicas para uma boa navegação.

5.2.Quais os problemas que envolvem os professores?

Além dos problemas mencionados anteriormente que podem envolver qualquer funcionário da instituição educacional, é preciso ainda preparar o professor para que esteja apto a levar seus conhecimentos para sala de aula e preparar o aluno para o novo modelo de sociedade que nos apresenta. A questão que muito nos preocupa é que a maioria ainda não está preparado para uma atuação como esta. É preciso que também estejam dispostos a aprender.

O que pode ser feito? A melhor solução é que as instituições educacionais tomem a iniciativa de capacitar seus professores a fim de que estejam aptos a atuarem sob estes novos parâmetros.

Recomendamos a elaboração de palestras e ou capacitação específica para docentes, bem como um material de apoio com dicas e boas práticas para o uso ético e legal dos meios digitais em sala de aula.

► Para ensinar é preciso aprender! ◄

5.3.Material didático e direitos autorais

É preciso fazer uso de um material específico para ensinar as novas questões trazidas pela tecnologia. Além disso, a Instituição deve revisar de uma maneira geral a todo seu processo atual de uso e aplicação de material didático, especialmente o elaborado por terceiros. Isso se aplica a todo material utilizado para o processo ensino aprendizagem, incluindo neste os livros, apostilas, artigos, mídias como powerpoint e outros.

Quais são os problemas? Com o avanço das tecnologias e o surgimento de novos suportes físicos para a criação intelectual, como por exemplo, a mídia digital possibilitou-se um compartilhamento de acesso aos materiais didáticos disponibilizados pelas instituições educacionais entre várias turmas e até mesmo entre unidades (filiais). Com isto, abre-se uma brecha para que os autores possam questionar o meio de disponibilização e utilização que não esteja expresso no contrato.

O que pode ser feito? Primeiro é preciso que a instituição estabeleça os padrões de desenvolvimento de material didático e de disponibilização, sendo necessário também que defina um modelo de contrato inserido nos novos parâmetros de proteção tecnológica. Definições como: contratação para desenvolver conteúdo específico, contrato de docência + horas para desenvolvimento de conteúdo.

A simples contratação docente, sem menção ao conteúdo, apenas obriga o professor a entrega do mesmo a seus alunos, que pode neste caso ser apenas de forma oral. Feito isto, será possível revisar todos os contratos já existentes e adequá-los a esta nova realidade.

► A Instituição não pode dar o mau exemplo! ◄

5.4.Proteção da marca da instituição

O que é a Marca na Sociedade Digital? Os avanços sociais e tecnológicos que passamos pelos últimos trinta anos mudaram drasticamente as formas de relacionamento e interação entre as pessoas. Quem antes se encontrava em um local distante, agora pode ser contatado em tempo real. Fronteiras de países podem ser facilmente atravessadas com o simples "clik" de um *mouse*. Uma pessoa em seu escritório ou casa pode ter tudo à sua mão através de compras online. Esses e muitos outros eventos compõem o que chamamos de **Sociedade Digital**.

De olho na lei

Faça um estudo sobre a Lei da Propriedade Intelectual (Lei nº 9.279/96) e conheça detalhadamente todas as condições e direitos reservados às marcas e patentes.

A projeção digital da marca de uma instituição Educacional reflete sua identidade e suas atitudes. É importante ter em mente que não há fronteiras e tudo que for publicado com a marca da instituição, será entendido como sua opinião.

Quais os problemas que essa nova visão da sociedade pode causar? Como qualquer outra grande mudança, a Sociedade Digital criou novos riscos e abusos nunca antes imaginados. Apesar das facilidades propiciadas pela informatização dos processos, foi facilitada também a ação de pessoas mal intencionadas ou, simplesmente, mal informadas.

Mesmo que a instituição educacional não disponibilize o serviço de comércio eletrônico, ou que seu website seja meramente institucional, ela pode estar sujeita a riscos e possíveis danos. Por exemplo, um simples copiar e colar de uma logomarca por terceiros pode causar prejuízo à imagem de seus negócios, veiculando informações errôneas, enganosas ou injustas sobre sua empresa.

A Sociedade Digital nos trouxe várias vantagens para a consolidação das marcas. Mas toda essa facilidade também ajuda para que nomes respeitados ou que ainda estão disputando uma posição no mercado sejam facilmente copiados e atacados. Para que isso não ocorra, existem regras de proteção legal da marca em ambientes digitais.

A construção de um site de uma instituição educacional, o envio de newsletters, de e-mails, a manutenção de banco de dados e outras ações necessitam de controles especiais e de um planejamento cuidadoso para que sejam evitadas contingências legais envolvendo uma reputação que foi construída com árduo esforço.

O que pode ser feito? O primeiro passo a ser tomado é a elaboração das regras que irão reger as relações da instituição com seus funcionários, colaboradores, fornecedores, parceiros, alunos e comunidades através do uso de ferramentas eletrônicas. Isso se faz com a criação de algumas Políticas e Termos específicos como Normas de Segurança da Informação para os empregados e colaboradores e código de conduta para o aluno, bem como com atualização das minutas de contrato de trabalho, de serviços, de matrícula, de parceria, todas com clausulas novas, adequadas a esta nova realidade jurídica e de riscos. Esses documentos determinam para as partes envolvidas quais são os limites na utilização dos recursos – tangíveis (computador, rede) e intangíveis (informação, marca, software) – da empresa.

Os usuários devem receber informações detalhadas sobre a forma correta de utilizar as ferramentas de trabalho tecnológicas, quais as responsabilidades de cada um dentro das leis vigentes. Isso abrange os limites de uso de um e-mail corporativo, de navegação na internet por empregado ou aluno nas dependências da instituição, de contratação através de meios eletrônicos, de quem é a autoria ou propriedade por determinado conteúdo ou código fonte, entre outros. Deve ficar claramente estabelecidas quais são as condutas consideradas corretas, e quais são as incorretas, bem como as possíveis penalidades para um eventual descumprimento das mesmas.

Além da criação das regras através destas Políticas, Termos e código de conduta do aluno é necessário o permanente controle dos meios eletrônicos internos e externos da empresa, que se dá através do monitoramento. Isso ocorre porque a Internet é um meio extremamente dinâmico e é preciso estar constantemente vigiando, principalmente para pegar o infrator com a "mão na máquina". Os casos mais comuns são o de vazamento de informação confidencial, concorrência desleal, mau uso da marca, queda de produtividade por mau uso da internet, uso pessoal do e-mail profissional que gera danos a terceiros e responsabilidade para a instituição, contaminação por vírus ou códigos maliciosos que geram perda de dados ou prejuízos ainda maiores, tanto para a instituição como para o profissional envolvido.

As instituições educacionais possuem uma responsabilidade ainda maior pela utilização dos meios digitais por seus alunos. Um conteúdo criado pode se espalhar em minutos pelo mundo inteiro, o que faz com que o planejamento jurídico tenha que ser preventivo, antes da situação ocorrer, até para que se tenha as provas adequadas para uma eventual defesa da empresa ou acusação de um infrator. É preciso preparar o terreno, colocar **vacinas legais** nos ambientes eletrônicos, planejar o armazenamento de dados dentro do ciclo de vida jurídico da informação para saber o que guardar e o que pode ser eliminado, desde logs e e-mails até documentos. A auditoria técnica-legal dos sistemas corporativos é de extrema importância para que seja garantido o uso correto das ferramentas e informações disponibilizadas.

Além disso, todas as medidas tomadas para a proteção digital da marca somente terão resultado positivo **com a educação do usuário**. É muito importante que cada funcionários, aluno e colaborador tenha consciência da importância do bom uso de sua ferramenta de trabalho que, se bem utilizada, beneficiará toda empresa bem como a vida pessoal do próprio usuário. **Casos mais comuns de uso indevido da marca das Instituições Educacionais:**

- Comunidades online e/ou Websites do tipo "Eu odeio a escola X" tanto por terceiros, como até por funcionários ou ex-funcionários, alunos e/ou ex-alunos;
- Comunidades online e/ou Blogs que relatam o cotidiano de funcionários e alunos, divulgando inadvertidamente informações sigilosas ou indevidas;
- Uso da imagem, reputação e identidade visual da empresa para validar e-mails fraudulentos;
- Uso da marca da instituição por concorrente em ambientes de Internet, especialmente nos buscadores, através de palavras-chave e/ou links patrocinados, em que ao colocar o nome da empresa aparece uma publicidade do concorrente ou se é direcionado para o site do mesmo.

► Filmes no You Tube gravados dentro da escola podem gerar responsabilidades! ◄

Políticas e termos

As políticas e termos mais comuns para dar o devido tratamento jurídico às relações atuais com uso de tecnologia são:

- Política de uso de Ferramentas Tecnológicas pelas Equipes (e-mail, rede, intranet, extranet, internet, home Office, celular, palm, outros);
- Política de Privacidade;
- Política de Segurança da Informação;
- Política de uso de e-mail marketing;
- Política de GED – Gestão Eletrônica de documentos;
- Termo de Responsabilidade (em especial para TI);
- Termo de uso de Assinatura ou Certificado Digital;
- Termo de Proteção de Direitos Autorais;
- Acordo de Confidencialidade, outros;
- Código de Conduta do Aluno;
- Normas de Conduta e Procedimentos para EAD.

5.5.Registro de domínios

O que é um domínio? O primeiro passo para uma instituição educacional que quer entrar no mundo virtual, seja para divulgação ou para oferecimento de cursos a distância, é a construção de um site. Layout, hospedagem, manutenção, sistemas de gerenciamento de cursos e outras preocupações são essenciais para que o negócio ande bem, mas antes de tudo isso, é necessário pensar em um detalhe muito importante: o domínio.

O domínio representa o nome da sua empresa no mundo virtual. É o **www.nome.com.br e ou www.nome.edu.br**. Ele pode ser composto pelo nome de sua empresa ou por algum termo relacionado ao seu negócio, como www.educacao.com.br. É interessante que você escolha um endereço que seja facilmente memorizado pela clientela e que tenha uma grafia simples, para evitar erros de digitação.

O domínio é na verdade um território de valor que associa o conjunto de marca ou nome memorável com o de ponto comercial, daí a sua importância, pois há só um. É fundamental, independente do registro do domínio, fazer o registro de marca também quando for o caso.

O que pode acontecer? Quanto melhor a reputação de uma instituição educacional, mais suscetível ela se torna a golpes virtuais. É muito comum que um e-mail fraudulento se propague pela rede prometendo vantagens em nome de uma instituição conceituada. O golpe torna-se mais convincente ainda se a mensagem redireciona o usuário a algum site com endereço semelhante ao da instituição vítima.

O usuário distraído (a segunda vítima) muitas vezes acredita que o domínio indicado é realmente idôneo e ali coloca seus dados pessoais que, posteriormente, serão utilizados sem autorização. Essa prática maliciosa é conhecida como *cybersquatting e, apesar dos esforços de várias organizações, ela tem sido constantem*ente praticada pelo mundo todo.

Uma outra finalidade para o *cybersquatting* é o redirecionamento de usuários que digitaram um endereço de forma errada para sites de conteúdo alheio aos interesses da instituição. Esse conteúdo pode ser de cunho pornográfico, ilícito ou, até mesmo, sites que criticam a instituição de domínio semelhante.

Como conhecer e solucionar o problema? A sua instituição já tem um domínio registrado. Mas será que isso é o suficiente? Quanto mais conhecidos seus negócios, mais eles estarão sujeitos a fraudes e abusos de marca. Isso faz com que você repense se apenas um domínio é suficiente para sua proteção digital.

Antes de tudo, verifique se você é vítima do *cybersquatting*. Para endereços no Brasil, acesse www.registro.br e procure por domínios com grafia ou sonoridade semelhantes ao nome de suas marcas. Faça o mesmo para sites internacionais pelo endereço www.centralops.net/co e clique em *Domain Dossier*.

Se já existem endereços registrados que utilizam o nome de sua instituição, pode ser feita uma **disputa de domínios**. Existem três maneiras principais de disputa: um acordo extrajudicial feito entre a empresa, no caso a instituição educacional e o detentor do endereço, o pedido de transferência obrigatória por ordem judicial ou a decisão de um árbitro do WIPO e ICANN, muitas vezes utilizadas em disputas internacionais, principalmente em domínios.*com.*

Você sabia que um website é considerado obra no Brasil?

Além dos seus domínios, é aconselhável que você registre as principais interfaces gráficas do seu site junto à Biblioteca Nacional. Essa medida garante que sua identidade visual não seja utilizada por terceiros, protegendo seus direitos autorais.

É interessante que você registre domínios com sons semelhantes ao nome da sua instituição para evitar que quem digite de forma incorreta acabe caindo em armadilhas, isso é chamado de "domínios anti-fraude". Também é recomendado registrar o domínio *.com* (sem o *.br*), que tem sido muito procurado por fraudadores. Esta gestão de domínios é uma estratégia preventiva para evitar riscos e responsabilidades legais.

5.6.O website da instituição educacional

Colocar um site no ar exige muitos cuidados para que a instituição esteja de acordo com as leis brasileiras, especialmente o Novo Código Civil, o ECA e a própria Constituição Federal, além de outras normas. Esta adequação jurídica evita que a instituição sofra sanções legais, tendo prejuízos e desagradando seus clientes.

Toda empresa que hoje coloca um site na Internet já nasce globalizada, sujeita a uma série de normas e princípios de direito digital. É preciso estar atento. Ser responsável pela educação do usuário também. Na era do conhecimento, o desconhecimento legal, a omissão e a falta de visão jurídica pode ser fatal.

Sendo assim, primeiramente, é recomendável que a página exiba informações e documentos que explicitem a boa-fé de seus negócios, transmitindo confiança e transparência para a instituição. Veja os principais textos que o seu site deve conter:

a) Política de Privacidade

Se seu site obtém dados dos usuários através de cookies, formulários, enquetes ou de qualquer outro meio, é necessário um documento que deixe claro como será feito o uso dessas informações. É direito do usuário saber o motivo da coleta e o destino de seus dados. Mesmo que você não tenha cadastro na internet, mas faça uso de cadastro por cupons ou outros suportes físicos de mala direta, revistas, entre outros, como tudo isso ao final vira um banco de dados eletrônico, é importante ser transparente e publicar a política no site da instituição. Informações essenciais que uma Política de Privacidade deve conter:

- Nome e CNPJ da instituição que coleta os dados;
- Endereço físico, telefone e e-mail para contato;
- Empresas que compartilham os dados coletados no site;
- Finalidades da coleta de informações;
- Possibilidade de o próprio usuário alterar ou excluir seus dados;
- Responsabilidade do próprio usuário pela inserção de dados falsos ou imprecisos;
- Em caso de instituição que atue com menores de 14 anos, deve fornecer um formulário especial que deve conter autorização e forma de contato dos pais ou responsáveis legais da criança.

b) Termos de Uso de Serviços e de Direitos Autorais

Através dos Termos de Uso de Serviços, o usuário terá acesso às condições de navegação pelo site, o que ele pode ou não fazer, quais os limites de responsabilidade da instituição sobre o que consta no site. Devem ser mencionados os navegadores compatíveis, plugins necessários, resolução recomendada, indicação das demais políticas do site e todas as condições de uso do mesmo.

O Termo de Direitos Autorais estabelece limites de uso e armazenamento das informações e imagens veiculadas a fim de proteger os direitos autorais de seus titulares, quer sejam da instituição ou de terceiros, muito comum quando se faz uso de conteúdos desenvolvidos por outros ou em parceria, bem como links.

c) Metadados

São informações técnicas que compõem um arquivo eletrônico, indo além do dado principal, como, por exemplo, data de criação, nota de direitos autorais, site de origem, a informação de dimensões que é essencial caso a foto seja meramente ilustrativa, entre outras. Todas as imagens, documentos e demais arquivos do site devem possuir esses metadados, para que não existam dúvidas sobre procedência, uso permitido, autenticidade e demais características das informações, bens e serviços prestados por sua empresa.

d) Creative Commons

É uma padronização de contrato/ licença de uso que disponibiliza um selo que remete o usuário a uma página especial, que estabelece os limites de uso dos materiais disponibilizados, como uso comercial ou edição por parte de terceiros. Se seu site disponibiliza textos, vídeos, imagens ou qualquer outro tipo de conteúdo que você deseja autorizar o uso e limitar as responsabilidades da instituição, esta é uma alternativa interessante que incentiva o respeito a direitos autorais e a disseminação correta de informação.

5.7. Segurança da informação (SI)

O patrimônio e a identidade dos indivíduos e das empresas está em dados, por isso, segurança da informação é fundamental!

A melhor forma de garantir a integridade, confidencialidade e disponibilidade das informações que trafegam por seus sistemas é a elaboração de um documento que determine os usos autorizados e também os vetados de todos seus recursos. Este documento é chamado de Política de Segurança da Informação, que esclarece detalhadamente as normas da empresa a todos os seus colaboradores, a fim de evitar futuras contingências legais.

Para que não permaneçam dúvidas sobre as condutas da instituição, é necessário que todas as regras de segurança e de boas práticas sejam colocadas por escrito. Todas as orientações desse capítulo sobre Equipe devem ser documentadas e rigidamente obedecidas. Além disso, recomendamos colocar estas regras nas próprias interfaces gráficas, nos rodapés de e-mail, no log-in de entrada na rede, com avisos de sistema, principalmente para deixar claro que o ambiente está sujeito a monitoramento.

Atualmente existe uma série de normas e regulamentações internacionais que exigem a aplicação de boas práticas de segurança da informação nas empresas, tanto aquelas com negócios no Brasil como as que desejam se relacionar com bancos e outras entidades estrangeiras.

Principais normas internacionais relacionadas com a Segurança da Informação

ISO/IEC 17799:2005 – *Segurança da Informação*

ISO/IEC 27010 – *Sistema de Gestão de Segurança da Informação*

ISO/IEC 18044 – *Gestão Incidente Segurança da Informação*

Quais são as principais condutas de preservação da segurança?

- *Descarte seguro de mídias*

Grande parte dos vazamentos de informações sensíveis ocorre devido o descarte mal-feito das mídias utilizadas. O lixo de uma empresa pode revelar documentos confidencias e estratégias que poderiam ter sido protegidos com cuidados especiais de descarte. Os colaboradores devem ser orientados a apagar todos os dados antes de se desfazerem de um CD, disquete, papel, etc. Caso contrário, qualquer pessoa que revire o lixo da empresa terá acesso a dados valiosos que não deveriam ter se tornado públicos.

- *Combate à engenharia social*

O colaborador deve ser orientado a criar senha segura, bem como mantê-la de forma efetivamente protegida, sem anotá-la em lembretes próximos ao computador ou divulgá-las a colegas de trabalho. O usuário também deve ser orientado a não cair em abordagens maliciosas com o intuito de obter informações da empresa, já que isso pode inclusive trazer riscos para ele pessoalmente. Essas aproximações incluem ligações telefônicas de pessoas alheias ao negócio que solicitam senhas e outros dados (as vezes até se fazendo passar por alguém do TI ou do Suporte), galanteios, falsos chamados de emergência – que são urgentes demais para uma identificação mais detalhada – e qualquer outra forma de ludibriar ou enfraquecer a guarda da equipe, que, apenas pela confiança, concede alguma informação confidencial.

Leis do Trabalho

A Consolidação das Leis do Trabalho (CLT) trata das relações entre funcionários e contratantes, devendo ser de conhecimento obrigatório de todos. Veja o artigo abaixo, o qual cita um dos motivos de justa causa para que um funcionário tenha seu contrato rescindido:

Artigo 482 - Constituem justa causa para rescisão do contrato de trabalho pelo empregador: (...) g) violação de segredo da empresa;

Participação em blogs, fotologs e comunidades virtuais

Os colaboradores também devem ser orientados a não construir ou participar de blogs, fotologs e comunidades virtuais (ex. Orkut) que tratem de assuntos da instituição ou se o fizerem, devem estar atentos. Essa medida evita que informações confidenciais ou estratégicas sejam divulgadas, já que esses meios online são muito utilizados por terceiros mal intencionados, principalmente para difamação.

- *Uso correto de e-mail*

Um dos assuntos mais delicados na Política de Segurança da Informação é sobre o uso de e-mail corporativo e de e-mail pessoal ou para finalidade pessoal. É preciso que as normas sejam muito claras, para que elas sejam efetivamente observadas, juntamente com as leis vigentes.

É necessário que fique muito bem claro que a conta @suainstituicao.com.br e/ou conta @suainstituicao.xxx.br deve ser de uso estritamente profissional, pois sem isso a empresa passa a não estar legitimada para acessar suas próprias informações e contas de e-mail. Para fins pessoais, o colaborador deverá ter uma conta própria de e-mail, ficando a cargo da instituição analisar se este acesso será autorizado dentro do ambiente de trabalho, já que a grande maioria dos vírus são espalhados em e-mails pessoais.

Vale ressaltar que qualquer e-mail enviado pela conta corporativa é de responsabilidade da Instituição que passa a responder pelo conteúdo escrito no mesmo. O correio

eletrônico é uma ferramenta de trabalho como outra qualquer, cabe ao empregador definir o correto uso do mesmo.

- *Trabalho remoto adequado (home-office)*

  Muitas vezes é necessário que o professor exerça suas atividades fora dos limites físicos da empresa, como em casa – o chamado Home Office –, ou em um cyber-café. O usuário deve ser orientado para que, em caso de trabalho remoto, redobre seus cuidados quanto à Segurança da Informação.

  Deve ser obrigatório, por exemplo, o log off após o uso de máquinas compartilhadas, bem como a eliminação de arquivos utilizados, cookies (pequenos arquivos utilizados para identificar o usuário e suas preferências) e qualquer outro elemento que possa prejudicar a integridade das informações corporativas.

  Além disso, é necessário que a empresa autorize de maneira formal o trabalho remoto apenas a usuários que realmente necessitam do benefício, reservando-se o direito de suspendê-lo a qualquer momento, sem necessidade de prévia notificação.

  A forma de contratar serviços de acesso a internet, como banda larga, na casa do funcionário também precisam de um procedimento apropriado, para que outras coisas que sejam feitas neste ambiente não gerem responsabilidade para a empresa, mesmo quando não estiver relacionado a trabalho.

- *Ferramentas de Segurança*

  O colaborador deve ser orientado a fazer uso correto das ferramentas de segurança disponíveis. Devem ser instalados e constantemente atualizados, programas de proteção antivírus como firewalls e anti-spam.

  Apesar de impedirem a execução correta de certos e-mails ou websites, deve ser expressamente vetada a desativação dessas ferramentas, o que poderia implicar em brechas de segurança, expondo todas as máquinas a sérios danos e vazamento de informações.

- *Níveis de acesso corretamente estabelecidos*

  De acordo com o cargo exercido na instituição e as necessidades de cada função, os colaboradores poderão ter níveis diferenciados de acesso. A política deve ser clara ao conferir esses graus de privilégio, lembrando que, quanto mais alto o nível, maior deve ser a responsabilidade do usuário e mais severas serão as punições em caso de infrações.

- *Comitê de segurança*

  A instituição deve criar um grupo composto por profissionais de diversas áreas internas, que será responsável pela implementação da Política de Segurança. Este comitê deverá criar normas futuras, incentivar condutas seguras, avaliar a situação da instituição e tomar qualquer iniciativa que aprimore o grau de segurança dos dados da empresa.

- *Punições eficientes*

  O descumprimento das normas estabelecidas pode ensejar em punições severas ao usuário, que podem variar de uma simples advertência a demissão por justa causa. Além de sanções internas, o colaborador também poderá estar sujeito a sanções judiciais, como cíveis e penais, resultando em pagamento de indenização, multa ou, até mesmo, prisão.

- *Monitoramento legal*

  O monitoramento dos recursos digitais da instituição está legalmente autorizado, desde que seja realizado de forma ética e cuidadosa, com aviso claro e expresso. Ele é necessário para que haja um controle maior sobre o uso das informações e recursos corporativos, já que a Justiça brasileira entende que a empresa é responsável pelo mau uso da tecnologia por seus empregados. Logo, é necessário que sejam monitoradas e guardadas as comunicações eletrônicas para fins de uso como prova na justiça, para embasar auditorias, investigações, perícias, etc.

Direitos constitucionais

A Constituição Federal estabelece limites, estruturas e garantias relativas a situações e a personalidade do cidadão. O Art. 5º é famoso por reunir grande parte dessas garantias, as quais devem sempre ser observadas, como por exemplo:

Artigo 5º - (...)
X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;
XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal;
LVI - são inadmissíveis, no processo, as provas obtidas por meios ilícitos;

Para que isso seja feito da maneira correta, sem atacar o direito constitucional à privacidade de terceiros, é necessário que todos os usuários sejam alertados da existência dessa vigilância. A não ser que estejamos nos referindo a espaços públicos e abertos, há uma presunção de privacidade. Ou seja, se não for dito que não é privativo, ou que está sendo monitorado, entende-se que há privacidade.

Por isso, é fundamental que sempre haja um aviso legal de que o ambiente não é privativo. Ou seja, o aviso deve ser prévio e feito no próprio meio para garantir que a pessoa foi informada e tinha ciência de que tudo que estivesse fazendo estaria sujeito à observância de terceiros. Além desse aviso inicial, é recomendável que o sistema da empresa lembre, periodicamente, o usuário a respeito do monitoramento através de mensagens no sistema e em rodapés de e-mails.

- *Campanhas de Segurança*

  Mesmo possuindo uma Política de Segurança sólida, a instituição deve promover periodicamente campanhas que visem reforçar nos colaboradores a idéia de que todos são responsáveis pela proteção dos dados da empresa. Palestras e cartilhas são recursos excelentes para a ampla divulgação das normas e condutas da empresa.

5.8. Os bancos de dados e a gestão eletrônica de documentos

Com a informatização dos processos, os dados contidos nos sistemas corporativos se tornaram indispensáveis para o bom andamento dos negócios, já que reúnem praticamente tudo que a instituição e qualquer outra empresa necessita para levantamento de estatísticas, fidelização de clientela, contatos e demais recursos estratégicos. Toda a vida da instituição está em dados. Ou seja, os bancos de dados são mais que um ativo em termos de valor e de riqueza, são a prova jurídica das obrigações e relações da mesma.

Informações sobre alunos, professores, material didático, notas, processos, planos, orçamentos, logs, históricos e demais acervos formam bancos de dados, que atualmente representam um valioso ativo intangível de negócio, tão importante quanto a própria marca.

Quais os problemas? Como tudo de valor, os bancos de dados são alvos de interesses de terceiros e, se perdidos, podem gerar grandes prejuízos para a instituição. Além da perda dessas informações, pode também incidir responsabilidade civil pela guarda mal feita de dados de clientes ou terceiros. Imagine o transtorno quando informações pessoais de alunos menores de 14 anos são furtadas. Os pais dos alunos confiaram suas informações a uma instituição que não soube guardá-las!

Além de pessoas mal intencionadas, a perda de dados pode ocorrer simplesmente através de uma falha no sistema, fazendo com que informações coletadas durante anos desapareçam, sem que possam ser recuperadas**. A guarda não adequada dos bancos de dados gera grandes riscos para a instituição.**

O que pode ser feito? Primeiro, é preciso planejamento com elaboração de um plano de gestão dos bancos de dados da instituição, tanto sob o aspecto técnico, como também jurídico. Isso envolve inclusive Planos de Contingência, uso de backups, de redundância, planejamento de armazenagem segura com empresas que possam fazer este tipo de serviço. Assim como também a **criação de uma Política de Classificação da Informação** que determine o que deve ser guardado com maior cuidado e proteção, por serem dados confidenciais ou sensíveis, o que pode ser descartado, o que será usado como prova legal no futuro em questão trabalhista, civil, fiscal.

Além disso, para que dados confidenciais não sejam divulgados inapropriadamente, é necessário o monitoramento constante das atividades digitais através de programas específicos, bem como a aplicação de um acesso diferenciado de usuários, por alçadas e poderes, que exija níveis de autorização por usuário. Alguns só terão acesso para leitura, outros poderão editar, outros nem o acesso terão.

Prova legal

O Código de Processo Civil determina as regras a serem seguidas em processos judiciais, entre elas o uso das provas e evidências.

Veja o artigo abaixo:

Art. 332. Todos os meios legais, bem como os moralmente legítimos, ainda que não especificados neste Código, são hábeis para provar a verdade dos fatos, em que se funda a ação ou a defesa.

A educação dos usuários é essencial, uma vez que todos precisam estar atentos para evitarem falhas humanas, bem como abordagem fraudulenta, com uso do que se chama engenharia social: onde o criminoso se aproveita da inocência de um funcionário para obter informações (como senhas e arquivos) que levem aos bancos de dados desejados.

Para falhas no sistema, além da realização de backup periódico, é aconselhável que seja contratado um seguro para os dados valiosos. Esse seguro indeniza a empresa caso as informações sejam perdidas.

É importante que sua instituição faça a guarda de documentos eletrônicos, como e-mails, registros de acessos a sites, logs, histórico de navegação, condições aceitas e quaisquer outros eventos relevantes, inclusive dados de IP. Essa documentação garante evidências e provas legais em disputas judiciais tanto para comprovação como isenção de responsabilidade, bem como estabelecimento de obrigações entre as partes envolvidas. Mas esta guarda deve ser feita de modo a preservar a integridade dos documentos, muitas vezes com aplicação de certificação digital, para que não seja discutida a validade da prova, ou alegado que a mesma tenha sido adulterada ao longo do tempo. Na sociedade digital, o arquivo eletrônico é o original, a versão impressa é mera cópia. Ou seja, o e-mail impresso é cópia, é preciso guardar no formato original, que permite perícia.

5.9.Certificação digital

É a metodologia utilizada para reconhecimento e autenticação de identidade através de uma assinatura digital. É composto por um arquivo eletrônico que pode ser armazenado em um computador específico ou em um dispositivo portátil para ser utilizado em várias máquinas.

Entre os mais utilizados, o e-CNPJ é o documento digital que garante a identidade de uma empresa ao realizar transações bancárias online, assinar e-mails ou fazer transações junto à Receita Federal

que só poderiam ser realizadas de forma presencial. Para tanto, deve ser escolhido um representante legal, que será o responsável pela assinatura digital da empresa e também por mantê-la de forma segura e confidencial. Com funções semelhantes, existe já para as pessoas físicas o e-CPF.

Uma das principais características da assinatura digital é o não repúdio, isto é, a presunção legal de que todos os atos ratificados por essa assinatura foram realmente praticados pelo seu legítimo portador. Por isso, é muito importante que o representante legal escolhido tenha consciência da importância e do valor que tem a certificação digital, não podendo emprestá-la a ninguém, em nenhuma circunstância, já que seu eventual mau uso recairá sobre o responsável devidamente constituído e sobre a empresa.

A assinatura digital é uma prova de autoria já aceita tanto na justiça brasileira como internacionalmente, representando a identidade digital do indivíduo, seja pessoa jurídica ou física.

5.10.Software legal

Todo computador corporativo necessita de um sistema operacional e demais softwares, que se encarregarão de desempenhar funções relativas às atividades da instituição.

Além disso, hoje já podemos encontrar vários softwares educacionais para utilização em sala de aula. Muitos programas possuem uma licença de uso, que deve ser paga ao seu desenvolvedor.

Quais são os problemas? O principal é a utilização ilegal de um software dentro da instituição, que pode ocorrer de duas formas principais: uso indevido de licença conferida a terceiros ou uso de programa devidamente licenciado, mas para fins diversos dos autorizados nos termos de uso. É comum nas instituições educacionais, professores instalarem programas nos laboratórios sem a devida averiguação de licença de uso. Nesses casos, os responsáveis pela instalação clandestina (quem comprou, quem instalou e quem mandou instalar) poderão estar cometendo crime contra direitos autorais. Ou seja, a instituição deve ter controle do que está sendo instalado nas máquinas, ou então corre o risco de responder civil e criminalmente, o que envolve desde a pessoa responsável pelo TI até o dono da empresa.

O que pode ser feito? Primeiramente é ter o controle do que está nas máquinas da instituição. Se você não pode ou não quer pagar por licenças, a recomendação é optar por programas de uso livre ou versões de teste, lembrando-se sempre de observar suas condições de uso, normalmente dispostas em textos no momento do download que são conhecidos como *disclaimers,* e que possuem validade jurídica. É sempre importante ler atentamente estes documentos.

Caso a instituição tenha uma área dedicada ao desenvolvimento de softwares ou terceirize sua produção, pode ser importante fazer o registro dos códigos-fonte junto ao INPI – Instituto Nacional de Propriedade Industrial – embora não obrigatório, mas recomendável, para garantir uma maior proteção legal, bem como a legítima propriedade dos mesmos, e evitar situações de discussão de infração autoral no caso de querer a instituição mudar de fornecedor, por exemplo, e o mesmo alegar então que o software é dele, e não da instituição, que seria se fosse objeto de encomenda.

Além disso, recomendamos que cláusulas contratuais específicas sobre direito autoral e código fonte devem ser inseridas também, para proteger ainda mais a instituição destes riscos legais. Reveja suas minutas atuais para analisar o quanto adequada sua instituição está nestas boas práticas de Direito Digital.

5.11.Aspectos legais da terceirização

Por que terceirizar? Para a redução de custos e utilização de mão de obra cada vez mais especializada, muitas empresas optam por contratar serviços de outras companhias que se encarregam de recrutar e treinar funcionários mais qualificados. A princípio, todos os encargos trabalhistas como 13º salário, férias e FGTS ficam por conta da empresa de terceirizados, o que alivia a folha de pagamento das contratantes.

As soluções tecnológicas de sua instituição também podem passar pelo processo de terceirização - como armazenamento de dados, hospedagem e manutenção de site e aluguel de equipamentos -, devendo prestar atenção às limitações legais e à real necessidade do negócio.

É muito importante cuidar da interface com fornecedor de forma correta para não incorrer em responsabilidade solidária. É preciso determinar em cada contrato o significado dos termos para evitar interpretações subjetivas ou distintas das acordadas na época da contratação.

Quais os pontos de atenção e suas soluções? A legislação trabalhista autoriza a terceirização de serviços em geral, especialmente de atividade-meio, sendo que há riscos no tocante a terceirização de atividade-fim dos negócios.

Apesar de não precisar arcar com as obrigações trabalhistas no caso de terceirização, o contratante deve verificar se o terceirizado cumpre corretamente com esses encargos e que isto esteja claramente disposto em contrato. Caso contrário, sua empresa poderá ser responsável por esses pagamentos referentes aos serviços contratados.

Além do aspecto legal, devem-se avaliar o risco operacional, a confidencialidade dos negócios e o grau de preparação da empresa contratada para planos de continuidade e de contingência e também assuntos como proteção de direitos autorais e de dados e segurança da informação, proteção de imagem, entre outros.

No momento da terceirização de serviços de tecnologia (TI) é de extrema importância que a empresa observe as condições de segurança, disponibilidade dos serviços (conhecido como SLAs), armazenamento de dados que eventualmente poderão ser utilizados como provas, confidencialidade das informações trocadas, existência de suporte técnico e qualquer outra garantia de que o serviço será prestado de forma correta, sem resultar em qualquer espécie de prejuízo.

Consulte especialistas, ouça recomendações de clientes, visite sites e escolha com muita atenção seus terceirizados, afinal você está contratando novas pessoas para cuidarem de setores de sua empresa para que você fique tranqüilo para dedicar sua atenção a áreas mais estratégicas.

Quais os principais riscos legais que envolvem a terceirização?

- Interrupções do serviço decorrentes de desastre natural, disputa trabalhista, falência do fornecedor, dependência de um único fornecedor, etc.;
- Atrasos de entregas por alta utilização da capacidade do fornecedor, baixa qualidade da produção, ou manipulação excessiva;
- Disputas legais envolvendo propriedade intelectual;
- Responsabilidade por danos causados;
- Não cumprimento de atividades do escopo do serviço contratado;
- Custo de Produção e capacidade fixa, sem flexibilidade de acordo com oscilações do mercado.

5.12. O novo modelo para o contrato de matrícula

O contrato de matrícula é o instrumento jurídico que determina as responsabilidades e obrigações entre a instituição educacional e seus alunos ou responsáveis quando for o caso, como por exemplo, condições de prestação de serviço e contra prestação pecuniária.

Quais são os problemas? Poucas instituições educacionais se preocupam com a atualização do contrato de matrícula no que se refere à utilização das tecnologias hoje disponibilizadas. Como uma instituição compromissada com a educação, é necessário que estejam sempre atualizadas com as novas ferramentas no sentido de apoio educacional, como blogs, chats, fóruns, comunidades e e-mails. No entanto, sem nenhum aviso ou autorização dos alunos ou pais quando necessário. Falta clareza e cláusulas específicas quanto à modalidade de contrato eletrônico para prestação de serviços educacionais.

O que pode ser feito? A atualização dos contratos é imprescindível para proteção da empresa. Clausulas indicativas de utilização das ferramentas tecnológicas e acesso à internet devem constar do contrato. Os pais, no caso de alunos menores de idade devem estar cientes de tal utilização, quanto aos demais, os alunos devem estar cientes de suas responsabilidades na utilização de tais ferramentas.

Para os contratos eletrônicos, também se deve atender aos mesmos dispositivos que regulamentam os contratos escritos, no entanto deve-se ficar atento às clausulas de privacidade na coleta de dados e outras indicações que possam garantir a total eficiência do contrato.

Os contratos de bens e serviços digitais devem possuir elementos nem sempre presentes nos contratos tradicionais. São questões e entendimentos que precisam ser acertados de forma precisa para que não ocorram interpretações equivocadas.

Um contrato eletrônico não possui uma forma rígida, como uma tela similar às folhas de papel comumente utilizado para tal instrumento. Um simples e-mail ou SMS (também conhecidos como torpedos de celular) podem resultar em obrigações, que devem ser cumpridas da mesma forma que os contratos de papel assinado a caneta. A manifestação de vontade é feita de maneira não presencial e é armazenada de modo digital ou físico, com uma impressão final. Veja as principais características necessárias para um contrato eletrônico:

- *Glossário*

  Muitos dos termos utilizados no mundo digital são bem recentes e, para muitas pessoas, eles são completamente desconhecidos. É por isso que todos os documentos que tratam sobre condutas, bens ou serviços digitais devem conter um glossário com a definição exata dos termos utilizados. É importante que não haja subjetividade ou interpretações prejudiciais perante o judiciário, caso surja alguma contingência legal.

- *Cláusula arbitral*

  Nosso ordenamento jurídico permite que as partes envolvidas se abstenham de recorrer à justiça tradicional para que seja utilizada a intervenção de um árbitro. A arbitragem pode não ser a solução mais barata para alguns conflitos, mas é uma opção mais rápida e que pode ser proferida por um profissional especializado no assunto, sem ter, necessariamente, uma formação jurídica.

- *Cláusula de prova eletrônica*

  Deve existir uma garantia contratual de que a troca de informações entre as partes por meio de todo e qualquer tipo de tecnologia possua validade com prova legal. São usualmente usados os e-mails que tratem de assuntos relativos a eficácia do contrato ou qualquer outra forma de comunicação virtual.

- *Cláusula de confidencialidade*

  As partes devem estabelecer proteção e sigilo às informações, dados ou conteúdos tidos como sensíveis, como informações que fazem parte do segredo comercial da empresa, dados pessoais de terceiros, normas internas, informações financeiras, estratégias de mercado e outras questões que mereçam ser protegidas.

- *Responsabilidades*

  Devem ser delineadas as responsabilidades de ambas as partes quanto à tecnologia adotada, segurança, formas de acesso, disponibilidade, atualizações, sigilo, direitos autorais e demais riscos envolvidos no negócio.

5.13.Contratos de trabalho

O contrato de trabalho é o instrumento jurídico pelo qual empregado e empregador definem as condições de trabalho e salário.

Quais são os problemas? A medida que o avanço tecnológico provoca mudanças comportamentais, é certo que seus efeitos atingem também a relação entre empregado e empregador. Portanto, assim como os contratos de matrícula, os contratos de trabalho se tornam obsoletos a medida que não atendem mais à realidade de uma sociedade conectada.

Com o surgimento de repositórios virtuais que permitem acompanhamento pedagógico bem como a entrega de cursos a distância como o e-learning, temos por conseqüência um novo modelo de relação professor aluno, o que exige uma reestruturação de tempo e dedicação independente de ser presencial ou não, o que pode acarretar problemas de ordem trabalhista. Outra questão já mencionada é quanto aos direitos autorais de material desenvolvido durante o vinculo empregatício.

O que pode ser feito? A melhor solução é a reestruturação do contrato de trabalho dos professores, inserindo clausulas específicas sobre acompanhamento online de uma turma ou ainda aulas em cursos inteiramente online, resposta a e-mails de alunos entre outros.

- *Cláusula de aceite da Política de Segurança da Informação*

  O professor, funcionário ou colaborador, deve aceitar as condições da Política e Normas de segurança da Informação quando existirem, para tanto, aconselhamos que esteja previsto seu aceite no próprio contrato de trabalho.

- *Cláusula de prova eletrônica*

  Deve existir uma garantia contratual de que a troca de informações entre as partes por meio de todo e qualquer tipo de tecnologia possua validade com prova legal. São usualmente usados os e-mails que tratem de assuntos relativos a eficácia do contrato ou qualquer outra forma de comunicação virtual.

- *Cláusula de confidencialidade*

  As partes devem estabelecer proteção e sigilo às informações, dados ou conteúdos tidos como sensíveis, como informações que fazem parte do segredo comercial da empresa, dados pessoais de terceiros, normas internas, informações financeiras, estratégias de mercado e outras questões que mereçam ser protegidas.

- *Responsabilidades*

  Devem ser delineadas as responsabilidades de ambas as partes quanto à tecnologia adotada, segurança, formas de acesso, disponibilidade, atualizações, sigilo, direitos autorais e demais riscos envolvidos no negócio.

Problemas mais comuns enfrentados por lojas virtuais

- Pessoa que afirma não ter realizado a compra de curso que lhe é atribuída;
- Não recebimento de acesso ao produto (curso);
- Informação equivocada sobre preços ou características e datas do curso;
- Desvio de dados confidencias de clientes;
- Registro e guarda inadequada de evidências relacionadas ao negócio.

5.14.O novo modelo para contrato de venda de cursos online e e-learning

O comércio eletrônico (ou simplesmente o e-Commerce) tem se expandido no Brasil graças ao aprimoramento de qualidade das empresas do setor e também com a popularização da banda larga, o que aumenta o número de vistas e tempo de permanência nas lojas virtuais. Nosso país tem batido recordes sucessivos em tempo de conexão por usuário, o que motiva as lojas virtuais a tentar reter uma boa parcela de todo esse tempo navegado. O mesmo tem acontecido para vendas de cursos online. Principalmente na

venda de cursos para e-learning.

Como fica o consumidor? Ao montar um sistema de venda de cursos online, lembre-se que todos os direitos do consumidor são garantidos também no mundo virtual. Portanto, tenha muito cuidado ao ofertar seus bens e serviços, já que preços, entregas e características devem sempre ser honrados.

O Código de Defesa do Consumidor confere ao comprador virtual o direito de desistir da compra até sete dias depois do recebimento da mercadoria, portanto, qualquer disposição ao contrário estabelecida por sua instituição poderá ser considerada uma infração legal, podendo incidir sanções aplicadas pelos órgãos de proteção ao consumidor.

É muito importante que o site exiba de forma clara a área de abrangência de seus negócios, isto é, se você atende apenas sua cidade, estado, se faz entregas para todo o Brasil ou se você possui estrutura para atender o mundo inteiro. Se seus serviços forem de âmbito internacional, fique atento às normas locais, que devem sempre ser obedecidas.

Visite periodicamente sites que compilam reclamações de consumidores, como o www.reclameaqui.net. Assim, você pode aprimorar o controle interno de qualidade e também conhecer os pontos fracos da concorrência.

Direitos do consumidor

O Código de Defesa do Consumidor (CDC) reúne todas as condições essenciais que devem ser observadas antes, durante e depois de uma relação comercial. Ele também determina penas como multas e até mesmo detenção. Ele deve sempre ser respeitado para evitar transtornos legais de dissabores com seus clientes. Segundo o código, temos:

Art. 6º São direitos básicos do consumidor: (...)
III – a informação adequada e clara sobre os diferentes produtos e serviços, com especificação correta de quantidade, características, composição, qualidade e preço, bem como sobre os riscos que apresentam;

Quais os documentos indispensáveis? Na venda de cursos online também é necessária a exibição de uma Política de Privacidade consistente, que auxilie o consumidor a esclarecer dúvidas sobre a instituição. Transparência é o que rege os negócios online. Quando não é possível obter informações exatas sobre uma instituição, é natural que o consumidor opte por outro site.

Elabore também um documento que deixe bem clara a postura da instituição em relação à desistência ou troca de curso do qual se matriculou, devolução de valores já pagos, prazos e modalidades de entrega, características dos cursos, carga horária, forma de mediação, ferramentas disponibilizadas e formas de pagamento.

No momento da compra, é recomendável que seja enviado ao e-mail do cliente uma cópia de todos os termos do site, para que ele tome novamente ciência das regras da instituição. É preciso que deixe claro também, os documentos que devem ser entregues ou enviados à instituição em seu original.

Como realizar o atendimento ao cliente? Sempre esclareça dúvidas e esteja aberto a críticas! Mais do que deixar um cliente satisfeito, essa postura receptiva auxilia sua instituição a localizar e melhorar seus pontos fracos, aperfeiçoando cada vez mais seus serviços.

Invista em canais de comunicação. Disponibilize telefones, endereços físicos e e-mails para contato. A grande diferença entre um ambiente de atendimento físico e um virtual é que o primeiro está restrito aos horários convencionais de funcionamento. No e-Commerce não existe horário comercial, por isso invista em uma equipe disponível 24 horas por dia, 7 dias por semana. A melhor alternativa de comunicação é a implementação de uma chat no site da instituição, para que o usuário receba, a qualquer momento, informações de maneira instantânea.

O que é identidade visual? A identidade visual engloba todas as características de uma marca que são facilmente reconhecidas até mesmo se vistas de relance. Logotipo, desenhos, cores, frases e até mesmo fontes tipográficas e pessoas famosas podem compor os elementos de identificação de uma instituição.

Explore esses elementos e consolide a identidade visual de sua instituição, sempre a utilizando em materiais promocionais, banners, e-mails marketing e hot sites. Essa medida ajuda a prevenir fraudes eletrônicas que utilizam sua marca, já que dificulta a ação de fraudadores, fazendo com que suas mensagens falsas fiquem menos convincentes perante suas vítimas em potencial.

Como fica a segurança? Invista na segurança interna do ambiente virtual, providenciando selos de site seguro e criptografia para envio de dados sensíveis. No meio de tantas fraudes, a confiança em um site é o principal fator de escolha por parte do usuário.

È necessário registro de eventos? É importante que sejam guardados registros de acessos, compras, contatos e outras atividades no site. Esses registros, também conhecidos por logs, funcionam como documentos probatórios em litígios com consumidores ou em situações de fraudes e ataques.

6.Check-up rápido da situação de sua instituição

Faça o teste abaixo e descubra se sua instituição está de acordo com as boas práticas digitais.

1. Os contratos de matrícula e de trabalho estão atualizados com as clausulas adequadas à utilização dos recursos digitais?
☐ Sim ☐ Não

2. Sua instituição detém possui autorização dos pais para navegação na internet quando alunos menores de idade?
☐ Sim ☐ Não

3. Seus professores e funcionários praticam a internet legal?
☐ Sim ☐ Não

4. Os professores de sua instituição estão capacitados para trabalhar as questões éticas e legais em sala de aula?
☐ Sim ☐ Não

5. Foi implementada uma política por escrito que trate do uso das ferramentas de Tecnologia da Informação pelas equipes e seus colaboradores?
☐ Sim ☐ Não

6. Sua escola possui código de conduta do aluno?
☐ Sim ☐ Não

7. O site de sua empresa possui uma política de privacidade consistente?
☐ Sim ☐ Não

8. Os dados estão protegidos por uma política de segurança da informação?
☐ Sim ☐ Não

9. As páginas que coletam dados sensíveis possuem selo de site seguro?
☐ Sim ☐ Não

10. O site possui aviso de direitos autorais?
☐ Sim ☐ Não

11. Os softwares utilizados pela empresa foram obtidos de forma legal?
☐ Sim ☐ Não

Resultados:

Mais respostas Sim: Parabéns! Sua instituição está no caminho certo, mas não deixe de observar as questões que ainda não estão de acordo com as boas práticas de Segurança da Informação, para evitar riscos legais e garantir seu crescimento satisfazendo clientes e respeitando as normas adotadas internacionalmente.

Mais respostas Não: É necessário que você revise a postura de sua instituição perante normas legais e boas práticas digitais. Para esses assuntos, procure sempre a orientação de um advogado, preferencialmente com uma formação ligada à tecnologia.

7.Recomendações de leitura

- PECK, Patricia. **Direito Digital** – Ed. Saraiva;
- CHARLOT, Bernard. **Relação com o Saber, formação de Professores e Globalização** – Ed. Armed;
- TIFFIN, John. RAJASINGHAM, Lalita. **A Universidade Virtual e Global** – Ed. Armed;
- JOLIBERT, Josette e colaboradores. A**lém dos Muros da Escola** – Ed. Armed;
- MURCIA, Juan Antonio Moreno e colaboradores. **Aprendizagem através do Jogo** – Ed. Armed;
- Perrenoud, Philippe. THURLER, Mônica Gather. A**s Competências para ensinar no séc. XXI** – Ed. Armed;
- AMSTRONG, Alison. CASEMENT, Charles. **A Criança e a Máquina. Como computadores colocam a Educação de nossos filhos em risco** – Ed. Armed;
- SANCHO, Juana Maria (org). **Para uma Tecnologia Educacional** – Ed. Artmed;
- ELIAS, Roberto João. **Direitos Fundamentais da Criança e do Adolescente** – Editora Saraiva;
- ANDRADE, Ronaldo Alves de. **Contrato Eletrônico no Novo Código Civil e no Código do Consumidor**. Brochura: 2004;
- DE LUCCA, Newton. **Aspectos Jurídicos da Contratação Informática e Telemática** – Saraiva;
- SÊMOLA, Marcos. **Gestão da Segurança da Informação** – Ed. Campus;
- DIAS, Claudia. **Segurança e Auditoria da Tecnologia da Informação** – Ed. Axcel Books;
- MITNICK, Kevin D. SIMON, William L. **A Arte de Enganar** – Ed. Pearson Makron Books;
- MARTINS, Ives Gandra. PEREIRA Jr, Antonio Jorge (coords). **Direito à Privacidade** – Ed. Idéia e Letras;
- BARALDI, Paulo. **Gerenciamento de Risco** – Ed. Campus.
- FERREIRA, Fernbando Nicolau Freitas e Araújo, Márcio Tadeu. **Política de Segurança da Informação** – Ed. Ciência Moderna

PPP Advogados

Somos um escritório especializado em Direito Digital. Esta é uma nova área jurídica que exige conhecimento específico de tecnologia e que envolve questões multidisciplinares.

No Direito Digital as principais "testemunhas" são máquinas, servidores e sistemas. Assim, a prova legal passa a ser o arquivo eletrônico, que recebe o status de documento original – e qualquer versão impressa passa a ser meramente uma cópia. Isso muda toda a forma de lidar com a guarda da documentação das obrigações das empresas para uso futuro, principalmente em situações de discussão judicial.

Por isso, o Direito Digital exige visão estratégica e de prevenção, com aplicação transversal em todas as áreas do negócio, reunindo não só as leis vigentes, mas também criando novas regulamentações para tratar de temas como Identidade Digital (como uso de senhas, logins, assinatura e certificação digital) e proteção de bancos de dados (em conformidade com os preceitos de privacidade, protegidos pela Constituição Federal).

Possuímos escritório em São Paulo e assessoramos aproximadamente 42 clientes no Brasil (São Paulo, Rio de Janeiro, Brasília) e em âmbito internacional (especialmente América Latina). Já treinamos mais de 9.500 profissionais de diversas empresas em questões relacionadas a Segurança da Informação e Direito Digital.

Nosso principal diferencial é que somos ADVOGADOS QUE ENTENDEM DE TECNOLOGIA! Nossa visão é a de que QUANDO A SOCIEDADE MUDA, O DIREITO TAMBEM DEVE MUDAR!

Entendemos que a melhor blindagem jurídica é aplicar o principio do videogame, que usa lógica indutiva para PASSAR A REGRA DO JOGO, NO PROPRIO JOGO. Ou seja, programar a lei nos softwares, interfaces, e-mails, disclaimers, outros.

Prestamos assessoria técnica e legal, fornecendo aos nossos clientes todo apoio, experiência e conhecimento necessários para enfrentar os riscos e aproveitar as oportunidades trazidas pela Era Digital.

Nossos serviços podem ser contratados por projeto especifico, ou como uma assessoria mensal para apoiar a empresa na prevenção e solução de questões relacionadas ao uso de tecnologia e suas implicações legais.

■ ■ ■

Advogadas responsáveis pelo projeto

DRA. PATRICIA PECK PINHEIRO: sócia sênior da PPP Advogados**,** especialista em Direito Digital, formada pela Universidade de São Paulo, com especialização em negócios pela Harvard Business School e MBA em marketing pela Madia Marketing School. É autora do livro "Direito Digital" pela Editora Saraiva, além de participação nos livros e-Dicas e Internet Legal. É colunista do IDG Now e articulista da Gazeta Mercantil, Valor Econômico, Revista Executivos Financeiros, Info Exame, Info Corporate, About, Revista do Anunciante, Jornal Propaganda e Marketing, Meio & Mensagem, Telecom Negócios, Super Interessante, com participação em diversos programas entre eles Globonews, Espaço Aberto, entre outros. Com experiência internacional nos EUA, Portugal, Coréia, começou a trabalhar com tecnologia aos 13 anos, como programadora de games para o computador Atari, tendo tido uma BBS, assim como ainda adolescente montou seu próprio site chamado "Urbanoide.com.br", além de ter se aprofundado no estudo dos princípios de Lógica Indutiva. Este conhecimento é hoje aproveitado em suas recomendações para criação de vacinas legais eletrônicas e desenvolvimento de "software legal", como medida de prevenção na gestão do risco digital de seus clientes. Tem ministrado diversos treinamentos para o SENAC, ITA, ISSA, USP, UNICAMP, Sucesu-SP, OAB/SP, CNASI, Security Day/ISS, IPEN, ABA – Associação Brasileira de Anunciantes, entre outros.

DRA. CRISTINA SLEIMAN: Advogada e pedagoga, associada à PPP Advogados, formada em direito pela UNICAPITAL, mestranda na Escola Politécnica da Universidade de São Paulo, formada em pedagogia com habilitação em administração escolar pela Universidade São Judas Tadeu com especialização em Direito da tecnologia pela FGV/RJ, Curso de Extensão Educador Virtual no Senac em parceria com Simon Fraser University (Canadá). Possui experiência em desenvolvimento de cursos de EAD, programação de sites em HTML, ASP e flash. Membro da Comissão do Advogado Professor da OAB/SP. Diretora executiva da APEJ – Associação dos Professores do Ensino Jurídico do Estado de São Paulo. Possui vasta experiência em capacitação de docentes, vem desenvolvendo um trabalho de conscientização do uso responsável das ferramentas disponibilizadas hoje, pelas novas tecnologias. Atuou no Senac São Paulo na Gerência de Desenvolvimento Educacional como Supervisora educacional e no Projeto de Uso de Novas Tecnologias de Informação e Comunicação em Educação e posteriormente na Gerência de Sistemas na elaboração da Política e Normas de Segurança da Informação.

■ ■ ■

Rua Alves Guimarães, 462, Conj. 63, Pinheiros, São Paulo-SP, 05410-000 Tel./FAX: 55 11 3068-0777
E-mail: **CONTATO@PPPADVOGADOS.COM.BR** Site: **WWW.PPPADVOGADOS.COM.BR**