CARTILHA INSTITUCIONAL DE SEGURANÇA DA INFORMAÇÃO E PREVENÇÃO A FRAUDES

ASSOCIAÇÃO BRASILEIRA DE AGÊNCIAS DE PUBLICIDADE

A cartilha elaborada pelo Dr. Rony Vainzof, do escritório Opice Blum, é bastante didática, sintética e objetiva.

Relaciona os principais problemas que o mundo virtual pode causar às pessoas físicas e jurídicas e às agências que trabalham com informações altamente confidenciais de seus clientes e estão sempre sujeitas à quebra das regras de sigilo firmadas.

Portanto, entendo que essa cartilha é um ABC de como as agências devem se acautelar quanto às informações que obtém e que dispõem a terceiros, para reduzir os riscos de danos incomensuráveis.

Paulo Gomes de Oliveira Filho
Consultor Jurídico da ABAP

As inovações tecnológicas facultaram novas formas de interação entre as pessoas, tanto em suas vidas pessoais quanto profissionais, influenciando de forma significativa o modo como as pessoas se comunicam, como armazenam seus documentos e informações considerados relevantes - ou até mesmo sigilosos - e, ainda, a forma como desempenham suas atividades profissionais.

Contudo, em que pesem todas as vantagens relacionadas ao emprego de meios digitais na vida cotidiana, sua utilização também acarreta diversos riscos, tais como: furto de dados e de informações sigilosas, invasão de privacidade, golpes e fraudes, exposição de sistemas a códigos maliciosos, a estes não se limitando. Certo é que todos esses incidentes podem colocar em risco não apenas dados pessoais de usuários, como informações sensíveis pertencentes a empresas, extrapolando, inclusive, os meios digitais e se perpetrando fora destes.

O objetivo desta Cartilha, portanto, é orientar as agências de publicidade vinculadas à Associação Brasileira de Agências de Publicidade - ABAP e seus colaboradores sobre as melhores práticas preventivas a serem adotadas para sua proteção em ambiente virtual, buscando sempre garantir a confidencialidade, integridade, disponibilidade e autenticidade de suas informações. Desse modo, a leitura do presente documento é altamente recomendada para todos aqueles que utilizam meios eletrônicos e Internet em seu cotidiano.

Rony Vainzof
Opice Blum

SUMÁRIO

1. SEGURANÇA DAS INFORMAÇÕES E DE DADOS PESSOAIS

1.1 Segurança de Senhas

As senhas permitem a autenticação do usuário quando do acesso às suas contas nas mais diversas plataformas e dispositivos eletrônicos no meio corporativo, garantindo que apenas pessoas autorizadas tenham acesso a determinados equipamentos e informações, validando a identidade e autenticando o usuário para assegurar sua legitimidade de acesso.

Diante da relevância da utilização adequada das senhas para a proteção de informações, é fundamental a escolha e utilização de senhas seguras em suas contas e dispositivos eletrônicos, sendo recomendável a atuação das empresas no sentido de exigi-las em todas as ferramentas corporativas.

Senhas óbvias, tais como: datas de aniversário, placas de veículos ou nomes de filhos, bem como combinações numéricas ou alfanuméricas comuns – tais como “123456”, “4321abcd” - não são seguras e podem facilmente serem descobertas por pessoas ou programas decodificadores de senhas.

Para criar uma senha segura é recomendável que os Colaboradores observem as seguintes instruções:

- ✓ As senhas devem ser compostas por, no mínimo, 8 (oito) caracteres;
- ✓ Suas senhas devem ser alteradas com frequência e nunca devem ser repetidas senhas utilizadas anteriormente; e
- ✓ Fiquem atentos a informações sobre vazamento de dados de determinados serviços. Se houver esse tipo de ocorrência, em um serviço utilizado, modifiquem as credenciais de acesso, para evitar que dados sejam obtidos por terceiros.

- × Não utilizem apenas letras ou números. Senhas seguras devem conter letras maiúsculas e minúsculas, números e caracteres não alfanuméricos (tais como @, $, # etc.);
- × Não componham suas senhas com seus nomes e/ou sobrenomes, nome da empresa em que trabalham ou qualquer variação desse tipo;

- Não utilizem a mesma senha para todas as contas, especialmente senhas utilizadas em contas corporativas. Dessa forma, se alguém descobrir uma das senhas do usuário, não conseguirá acessar todos os serviços em que este possui cadastro; e
- Nunca informem sua senha a terceiros, nem as anotem em papel ou em arquivos digitais, ou as incluam em processo automático de acesso ao sistema. Senhas devem ser sempre memorizadas e de uso estritamente pessoal, de modo a nunca serem compartilhadas com ou acessíveis por terceiros.

Em razão disso, recomenda-se que as empresas, a fim de assegurar a aplicação de tais medidas, estabeleçam as condições acima indicadas como critérios para seleção de senhas por meio da configuração de seus sistemas, impondo aos usuários que a escolha da senha obedeça às regras supracitadas.

1.2 Códigos Maliciosos

Códigos maliciosos, também denominados de *malwares*, são todos os tipos de programas que executam ações maliciosas em um *hardware* ou *software* em que forem instalados, podendo coletar informações confidenciais e apagar dados, causando danos incomensuráveis a usuários e empresas. Com o avanço da tecnologia, já existem *malwares* desenvolvidos para praticamente todos os dispositivos eletrônicos, não mais se limitando aos computadores, ou restritos a determinados sistemas operacionais.

Referidos códigos maliciosos podem se instalar nos dispositivos tecnológicos de várias maneiras, como, por exemplo, pela execução de arquivos infectados, pela exploração de vulnerabilidades existentes nos programas instalados, pela execução de mídias removíveis infectadas, como pen-drives, CDs e DVDs, bem como pela ação direta de usuários mal-intencionados, que invadem sistemas para a inserção de códigos maliciosos.

Existem diversos tipos de códigos maliciosos, como, por exemplo, mas não se limitando a: **(i)** vírus (programas maliciosos desenvolvidos para que se espalhem rapidamente, por meio de autorreplicação, quando da execução de arquivos); **(ii)** *worms* (semelhantes aos vírus, mas não dependem de interação

do usuário para serem ativados); **(iii)** *trojans* (códigos maliciosos escondidos em programas aparentemente legítimos, de modo que estes programas, ao serem executados, executam também funções danosas), **(iv**) *spywares* (programas de computador que possibilitam acompanhar diversas atividades realizadas em dado aparelho eletrônico, atuando por meio da coleta e envio de informações inseridas no dispositivo); **(v)** *bots* (programas que permitem que um dispositivo invadido seja controlado à distância, pelo invasor); **(vi)** *ransomwares* (códigos maliciosos que impedem o acesso ao sistema pela vítima, sendo conhecidos como "sequestradores" de dispositivos).

Para evitar a contaminação dos sistemas informáticos por códigos maliciosos, é recomendável que os usuários e as empresas adotem, no mínimo, as seguintes medidas:

- ✓ Mantenham sempre programas antivírus e *antispywares* atualizados em todos os sistemas e equipamentos, se possível, configurando-os para a realização de atualização automática, vez que muitos programas maliciosos se utilizam de vulnerabilidades do sistema que costumam ser corrigidas em atualizações;
- ✓ Mantenham os sistemas operacionais e os demais programas e aplicativos utilizados sempre atualizados, principalmente quando as atualizações corrigirem falhas de segurança;
- ✓ Utilizem programa *firewall* nos dispositivos informáticos utilizados, pois ele cria uma barreira entre o dispositivo e a Internet e, se bem configurado, é capaz de registrar tentativas de acesso indevido ao sistema, bloquear o envio de informações coletadas por códigos maliciosos para terceiros, bloquear tentativas de invasão ao sistema, filtrar códigos maliciosos, bem como evitar a propagação daqueles já instalados; e
- ✓ Instruam todos os usuários dos sistemas a não clicar em janelas *pop-up* e caixas de diálogo em *sites* não confiáveis, bem como a não remover ou modificar a ferramenta de detecção, prevenção e eliminação de códigos maliciosos.

- × Não abram anexos de e-mails não confiáveis ou de origem duvidosa;
- × Não cliquem em janelas *pop-up*, caixas de diálogo ou *hyperlinks* em *sites* não confiáveis; e

- Não instalem programas ou aplicativos de origem desconhecida ou não confiável.

Recomenda-se que, no âmbito corporativo, as atualizações do sistema e dos programas antivírus e *antispywares* sejam agendadas para momento em que os colaboradores não utilizem os equipamentos e que os equipamentos sejam configurados de modo que não seja possível aos usuários alterar as configurações e instalar novas aplicações.

Ainda, é recomendável que as empresas configurem bloqueios a sites e aplicativos suspeitos ou que sejam reconhecidos como possíveis fontes de *malwares*, bem como não permitam a instalação em seus sistemas de programas pelos usuários em geral, mas apenas pelo Departamento de Tecnologia da Informação, de modo a mitigar os riscos de execução de códigos maliciosos nos dispositivos informáticos da empresa.

1.3 Segurança de Redes Sem fio (Redes Wi-Fi)

Graças à difusão dos dispositivos eletrônicos portáteis, as redes sem fio - mais comumente conhecidas como redes Wi-Fi - são cada vez mais utilizadas, possibilitando o acesso à Internet por meio de ondas de rádio, sem necessidade de plugar o dispositivo em qualquer outro aparelho tecnológico.

Contudo, o uso de redes sem fio pode trazer diversos riscos à segurança de empresas e usuários, especialmente quando utilizada rede não protegida adequadamente. Neste caso, não apenas as empresas, mas também os usuários estão sujeitos a diversas ameaças, como, por exemplo: furtos de dados de dispositivos conectados à rede, sendo possível o acesso à integralidade dos arquivos neles armazenados.

Justamente por essa razão, recomenda-se que dispositivos que contenham arquivos e informações importantes não sejam conectados a redes sem fio desconhecidas, não sendo recomendada a realização de pagamentos ou a troca de informações confidenciais por meio de redes Wi-Fi não conhecidas, ou abertas.

Caso seja utilizada ou fornecida conexão sem fio pela empresa, as seguintes sugestões podem tornar a rede mais segura:

- ✓ Altere as senhas de administrador padrão e o *Service Set Identifier* (SSID), conhecido como “nome da rede”. Cada dispositivo sem fio vem com configurações padrões, que precisam ser alteradas, com o objetivo de evitar o livre acesso por parte de terceiros mal-intencionados;
- ✓ Utilize criptografia, pois a ausência dela pode permitir que qualquer pessoa mal-intencionada capture o tráfego e tenha acesso a todo o conteúdo que circula na rede, como e-mails, senhas e dados confidenciais;
- ✓ Utilize filtros de Endereço MAC (*Media Access Control*), o qual constitui o endereço único de dispositivo que se conecta a uma rede. Dessa forma, é possível que uma rede permita o acesso apenas aos endereços MAC liberados, ficando os demais bloqueados; e
- ✓ Caso a empresa disponibilize rede Wi-Fi para seus clientes, essa deve ser segregada da rede utilizada pelos Colaboradores da empresa.

- ✗ SSIDs não devem conter o nome do proprietário ou da empresa proprietária da rede, nem apresentar informações capazes de identificá-los, ou que identifique a área ou função da rede.

Lembre-se: Quando vários dispositivos se conectam a uma mesma rede, todos eles são identificados pelo mesmo número IP (*Internet Protocol*). Desse modo, caso alguém realize uma atividade ilícita, utilizando-se de rede que não possua verificação dos usuários que se conectam a ela, o proprietário da rede pode vir a ser responsabilizado pelos danos e ilícitos cometidos.

É importante, portanto, às empresas, adotar ferramentas que permitam a identificação dos usuários conectados à sua rede em determinado momento, de modo e mitigar o risco de que estas venham a ser responsabilizadas por atos ilícitos cometidos por terceiros.

1.4 *Spam*

A palavra *Spam* está relacionada a e-mails não solicitados, enviados a um grande número de destinatários, normalmente com fins publicitários. Embora aparentemente inofensivos, além do tempo perdido para exclusão dessas mensagens não solicitadas, elas podem causar outros problemas, tais como:

- Perda de informações contidas em mensagens importantes, vez que estas podem se ocultar no meio do grande volume de *spam* recebido, não sendo lidas no momento oportuno ou sendo excluídas por engano;
- Não recebimento de mensagens, vez que, em serviços com limite de espaço de armazenamento na caixa de entrada, o volume de *spam* pode impedir o recebimento de mensagens importantes até que a caixa seja esvaziada;
- Gastos extras, pela empresa, com armazenamento de informações em seus servidores; e
- Recebimento de conteúdo considerado impróprio ou ofensivo pelo usuário.

Para evitar o recebimento de *spam*, ou para diminuir a quantidade dessas mensagens indesejáveis, é recomendável que as empresas e seus usuários:

- ✓ Utilizem filtros de *spam*, fornecidos pela maioria dos serviços de e-mail;

- × Não forneçam endereços de e-mail, pessoal ou profissional, em situações para as quais ele não seja fundamental, não disponibilizando tais informações para acesso público em páginas na Internet; e
- × Não cliquem ou orientem os usuários a não clicar em *links* recebidos por meio de *spam*, vez que tal ação pode servir como confirmação de que o endereço de e-mail destinatário é válido.

Ademais, os colaboradores devem ser orientados a não utilizar o e-mail fornecido pela companhia para preenchimento de formulários, a não ser que seja estritamente necessário para fins profissionais e, neste caso, que tenham atenção ao preenchê-los, pois muitos apresentam a autorização de recebimento de propagandas selecionada como padrão.

1.5 Armazenamento em nuvem

O armazenamento em nuvem (*cloud computing*) traz uma série de vantagens a empresas e usuários, como a possibilidade de acessar um documento em qualquer lugar, utilizando-se de qualquer dispositivo, bem como a possibilidade de economizar espaço de armazenamento em *hardware*, reduzindo os custos das empresas com relação à manutenção de servidores. Não por outra razão, tornou-se uma tendência crescente no mercado atual.

No entanto, a utilização de serviços de armazenamento em nuvem pode trazer uma série de riscos, como furto ou perda de informações, em razão de vulnerabilidades do sistema. Para minimizar tais riscos, é recomendável a adoção, no mínimo, das seguintes precauções pelas empresas e seus usuários:

- ✓ Verifiquem os Termos de Uso e a Política de Privacidade e/ou o Contrato de Prestação de Serviços dos serviços de *cloud computing* utilizados, de modo a conhecer e analisar a forma como as empresas armazenarão os dados e arquivos, não utilizando determinado serviço que contrarie o esperado ou as regras de segurança da empresa;
- ✓ Orientem os Colaboradores a utilizarem exclusivamente os serviços de armazenamento em nuvem aprovados e autorizados pela empresa;
- ✓ Utilizem somente senhas de acesso seguras nos serviços de *cloud computing*, de modo a evitar o acesso indevido a documentos, seguindo as recomendações anteriormente sugeridas;
- ✓ Realizem *backup* dos arquivos armazenados em nuvem, de modo a evitar a perda de informações por falhas nos serviços de armazenamento, ou eventual impossibilidade de acesso aos arquivos, em razão de indisponibilidade temporária dos serviços; e
- ✓ Orientem os colaboradores a sempre averiguar se as normas aplicáveis da companhia autorizam que informações de caráter corporativo sejam armazenadas em nuvem.

- × Evitem armazenar documentos sigilosos e informações confidenciais da empresa em nuvem, principalmente por meio de serviços gratuitos, vez que falhas de segurança do serviço de armazenamento podem expor informações confidenciais a terceiros mal-intencionados, causando danos irreparáveis.

1.6 Ataques de Negação de Serviço

Também conhecidos como Ataques *Denial-of-Service* (Ataques DoS), consistem em ações que têm como objetivo fazer com que sistemas tenham dificuldade, ou mesmo sejam obstados de realizar suas tarefas. No entanto, o autor de tais ataques, ao invés de buscar infectar o alvo com códigos maliciosos, sobrecarrega os sistemas alvos, de modo que esse consuma todos os seus recursos, impedindo-os de fornecer os serviços.

Uma variação dos Ataques DoS são os Ataques *Distributed Denial of Service* (Ataques DDoS), por meio dos quais são utilizados até milhares de computadores zumbis, infectados com *malwares*, para impedir o funcionamento de determinados sistemas. São ataques de grandes proporções, que frequentemente fazem uso de *botnets*.

Ataques DoS são difíceis de combater, especialmente em razão das diferenças entre estruturas e recursos de servidores. No entanto, algumas dicas podem ser úteis à empresa para evitar ataques DoS a seus servidores:

- ✓ Utilize filtros em seus servidores que bloqueiem pacotes com endereços IP inválidos, conhecidos como *antispoofing*;
- ✓ Utilize *firewall* eficiente;
- ✓ Utilize Sistemas de Detecção e Prevenção de Intrusão (*Intrusion Detection System* – IDS e *Intrusion Prevention System* – IPS); e
- ✓ Estabeleça um plano de contingência em caso de ataques, considerando os efeitos de uma eventual indisponibilidade de sistema.

1.7 Boas práticas de segurança das informações e da imagem da empresa em meio digitais

Além do exposto anteriormente, apresentamos, a seguir, algumas recomendações adicionais com o intuito de preservar a segurança das informações armazenadas em dispositivos eletrônicos e a imagem da empresa na Internet.

Recomendações de segurança das informações em meio digital:

- ✓ Realize *backups* periódicos de documentos e informações, tendo em vista que códigos maliciosos e falhas de sistema podem levar a exclusão de dados e arquivos importantes. Além disso, deve-se considerar que, especialmente no caso do uso de dispositivos móveis, como *smartphones*, *tablets* e *laptops* por colaboradores, os equipamentos que contêm informações importantes podem ser furtados ou perdidos;
- ✓ Configure os dispositivos informáticos utilizados pelos usuários de modo que o acesso a eles se dê sempre por meio de senha segura, estabelecendo, ainda, regras para bloqueio de tela;
- ✓ Determine a necessidade de criptografar quaisquer documentos que contenham informações confidenciais ou de grande importância para o desenvolvimento das atividades da empresa, instruindo seus colaboradores a evitar trafegar com dispositivos contendo dados sigilosos;
- ✓ Não permita o envio de e-mails, mensagens de texto ou em chats contendo informações sigilosas, sendo preferível orientar o colaborador a conversar pessoalmente sobre o assunto, a depender da criticidade dos dados;
- ✓ Ao encaminhar dispositivos eletrônicos para assistência técnica, exclua, se possível, dados confidenciais e/ou sensíveis, para evitar seu acesso e divulgação por pessoas não autorizadas;
- ✓ Ao se desfazer de um dispositivo eletrônico, apague todas as informações nele contidas e restaure as configurações de fábrica; e
- ✓ Instrua seus colaboradores a utilizarem sempre conexões seguras.

Recomendações para proteção da imagem da empresa em meios digitais:

- ✓ Oriente seus colaboradores a serem cuidadosos com as informações divulgadas na Internet, especialmente em redes sociais;
- ✓ Esclareça seus colaboradores sobre os riscos relacionados à utilização de redes sociais, cujo uso inadequado pode prejudicar não só a imagem do colaborador, mas também da própria empresa; e
- ✓ Instrua seus colaboradores a nunca publicarem informações relacionadas à companhia na internet, bem como nunca realizar qualquer publicação em nome da empresa.

Além disso, oriente-os a não publicar imagens, fotos, vídeos ou sons captados no ambiente corporativo.

Destacamos que estas recomendações, bem como todo o teor desta Cartilha, buscam mitigar os riscos relacionados à segurança dos dados e das informações de empresas, devendo, para tanto, tais recomendações serem informadas a seus colaboradores.

Desse modo, a fim de propiciar o apoio e a cooperação de todos os envolvidos, recomenda-se a elaboração, pela empresa, de Política de Segurança da Informação adequada às necessidades da companhia, de modo a instruir os colaboradores acerca das melhores práticas para resguardar a segurança das informações da empresa.

2. MELHORES PRÁTICAS DE SEGURANÇA EM MEIOS DIGITAIS

Diante do quanto acima exposto e considerando, especificamente, os riscos existentes no ambiente corporativo, apresentamos a seguir algumas práticas de adoção recomendável para mitigar incidentes relacionados a segurança em meios digitais:

2.1 Regra de Segurança da Informação

É recomendável que toda empresa possua Regra Interna de Segurança da Informação, que regule a utilização, guarda e manuseio de todas as suas informações, sistemas e equipamentos por seus usuários e colaboradores, de modo a evitar a perda ou vazamento de informações importantes, bem como acessos não autorizados aos sistemas da empresa ou a infecção dos mesmos por vírus ou outros códigos maliciosos.

Tais regras devem definir, entre outros aspectos, o que são informações sigilosas, como elas devem ser tratadas, quem pode ter acesso à infraestrutura tecnológica da empresa, como ela deve ser utilizada etc., tendo por objetivo mitigar riscos e prejuízos à empresa, bem como sua responsabilização por atos de terceiros ou próprios, relacionados às providências por ela adotadas para a segurança de suas informações.

2.2 Criptografia

Criptografia consiste no ato de codificar dados, para que apenas pessoas autorizadas consigam ter acesso às informações. Atualmente, são utilizadas diversas formas de criptografia para a proteção de variados documentos, como a criptografia de chave simétrica, que utiliza chave única para codificar e decodificar a informação; ou a criptografia de chave assimétrica, também conhecida como chave pública/privada, vez que utiliza duas chaves, uma para codificar e outra para decodificar a informação. O método mais adequado a ser adotado depende das necessidades específicas de cada empresa, sendo recomendável a utilização, também, de duplo grau de autenticação.

Desse modo, é recomendável a utilização de métodos criptográficos para proteger documentos confidenciais, cujo conteúdo seja de grande importância para a empresa, de modo a garantir que apenas pessoas autorizadas tenham acesso a eles. Além de arquivos, é possível ainda criptografar mensagens de e-mail, também como forma de evitar o acesso de conteúdo sigiloso por terceiros não autorizados.

2.3 Sistemas de *backup*

Backup é a cópia de segurança de arquivos e dados, de modo que, em caso de perda das informações originais, elas possam ser restauradas, evitando grandes prejuízos à empresa, sendo, portanto, fundamental. Em situações ideais, o *backup* deve ser realizado em tempo real, de modo a garantir que não ocorrerá a perda de dados. No entanto, em caso de impossibilidade, é recomendável a realização de *backup*, no mínimo, diariamente.

Ainda, deve ser estabelecido pela empresa um período para a retenção dos *backups,* levando-se em conta o tipo de informação armazenada e a legislação existente aplicável de forma específica.

Ademais, é importante que as empresas realizem, de forma regular, testes com referidas cópias de segurança, de forma a garantir que as informações salvas possam ser restauradas e disponibilizadas sempre que necessário.

Em caso de panes e indisponibilidades nos sistemas da companhia, embora o *backup* permita recuperar as informações perdidas, o sistema ainda permanecerá inoperante, o que pode gerar prejuízos de considerável monta a uma empresa, inclusive inviabilizando suas atividades por certo período.

Desse modo, para evitar perdas ainda maiores em caso de falhas de sistema, é recomendável que as empresas possuam ferramentas conhecidas como *Backup* de Missão Crítica, também chamado de ambiente de *Disaster Recovery*. Missão Crítica constitui um ambiente tecnológico construído com o intuito de evitar a paralisação de serviços computacionais. Ou seja, é uma infraestrutura tecnológica que permite que, em caso de falha de sistema, ainda seja possível garantir a operação da empresa.

2.4 Monitoramento da Internet

É recomendável o monitoramento constante do nome e das marcas da empresa na Internet, de modo a identificar sua utilização indevida, inclusive para fins de fraudes. Tal monitoramento é realizado mediante a adoção de ferramentas específicas, que realizam a varredura automática da Internet e, inclusive, de determinados sites e redes sociais.

Como mencionado anteriormente, a realização de tal monitoramento pode evitar a ocorrência de fraudes relacionadas à empresa, o que pode mitigar o risco de que esta venha a ser responsabilizada por eventuais prejuízos sofridos pelos consumidores, perpetrados por terceiros pela utilização da marca e nome da empresa.

3. CHECK-LIST DE SEGURANÇA NOS MEIOS DIGITAIS

Este *check-list* tem por objetivo permitir que as empresas verifiquem se estão de acordo com as melhores práticas de segurança em ambiente digital:

- A empresa utiliza senhas seguras para acesso a todos os serviços e dispositivos eletrônicos que utiliza?

- ✓ Em caso negativo ou se estiver em dúvida, altere suas senhas, conforme descrito no Item 1.1 desta Cartilha.

- A empresa possui programas antivírus e *antispywares* atualizados em todos os equipamentos eletrônicos?
  - ✓ Em caso negativo, adquira tais programas ou atualize os que já possui.

- A empresa possui rede sem fio de conexão à Internet protegida?
  - ✓ Em caso negativo ou caso esteja em dúvida, altere as configurações de sua rede nos termos do Item 1.3 desta Cartilha.

- A empresa instrui seus colaboradores a verificar os termos de uso e a política de privacidade dos portais antes de acessá-los?
  - ✓ Em caso negativo ou caso esteja em dúvida, recomendamos que seus colaboradores sejam orientados a realizar prévia e completa leitura de todos os termos antes de aceitá-los quando estiverem utilizando dispositivos da empresa.

- A empresa armazena informações em nuvem (isto é, utilizando-se de *cloud computing*)?
  Em caso positivo:
  - ✓ Certifique-se dos termos do contrato firmado com o fornecedor, bem como que sua empresa não disponibilizará nenhuma informação confidencial; e
  - ✓ Instrua seus colaboradores a não armazenar informações confidenciais em serviços de *cloud computing*.

- A Empresa realiza *backup* periódico de seus arquivos, inclusive dos armazenados em nuvem?
  - ✓ Em caso negativo, adote tal prática, de modo a evitar a perda de informações importantes por falhas ou invasões de sistemas.

- A empresa utiliza redes sociais e está ciente da participação de seus colaboradores em referidas redes?

- ✓ Instrua seus colaboradores a nunca utilizar redes sociais para falar em nome da empresa, bem como nunca publicar informações referentes as atividades da empresa.

- A empresa possui Regra Interna de Segurança da Informação?
  - ✓ Em caso negativo, recomendamos que seja elaborado tal documento, com o objetivo de preservar a segurança dos sistemas da empresa, bem como de seus dados.

Lembre-se que, com relação aos meios digitais, a prevenção de danos é sempre mais eficiente que sua reparação, que pode não ser eficaz. Além disso, importante notar que certos riscos aos quais os usuários e as empresas ficam expostos, em razão da utilização dos meios eletrônicos no desenvolvimento de suas atividades, podem, além de prejuízos financeiros, gerar responsabilidade legal perante terceiros.

Adotando, a empresa, todas as cautelas pertinentes, no intuito de mitigar riscos envolvendo incidentes de segurança e fraudes, será mais facilmente demonstrada sua boa-fé em sua atuação no combate a ilícitos, o que pode inclusive ser causa de diminuição de eventual sanção a ser aplicada judicialmente.

Deste modo, é recomendável que a empresa e seus colaboradores procurem adotar sempre as melhores práticas possíveis de segurança quando da utilização dos meios eletrônicos.

Esta Cartilha tem como objetivo reduzir os riscos relacionados à utilização da Internet e de dispositivos eletrônicos e evitar prejuízos financeiros, bem como impactos negativos às imagens das companhias. No entanto, em razão das constantes inovações tecnológicas e pela própria natureza da Internet, não é possível garantir que a execução de todas as recomendações previstas nesta Cartilha eliminarão todos os riscos relacionados a utilização das tecnologias aqui mencionadas, sendo fundamental manter o documento sempre atualizado.

OPICE BLUM
OPICE BLUM | BRUNO | ABRUSIO | VAINZOF

Al. Joaquim Eugênio de Lima, 680 - Jardim Paulista
São Paulo/SP - CEP 01403-000 – Tel: (11) 2189-0061

ASSOCIAÇÃO BRASILEIRA DE AGÊNCIAS DE PUBLICIDADE
RUA PEDROSO ALVARENGA, 1208 – 8º - ITAIM BIBI – SÃO PAULO – SP
04531-004 – TELEFONE: (11) 3074-2160 – www.abapnacional.com.br