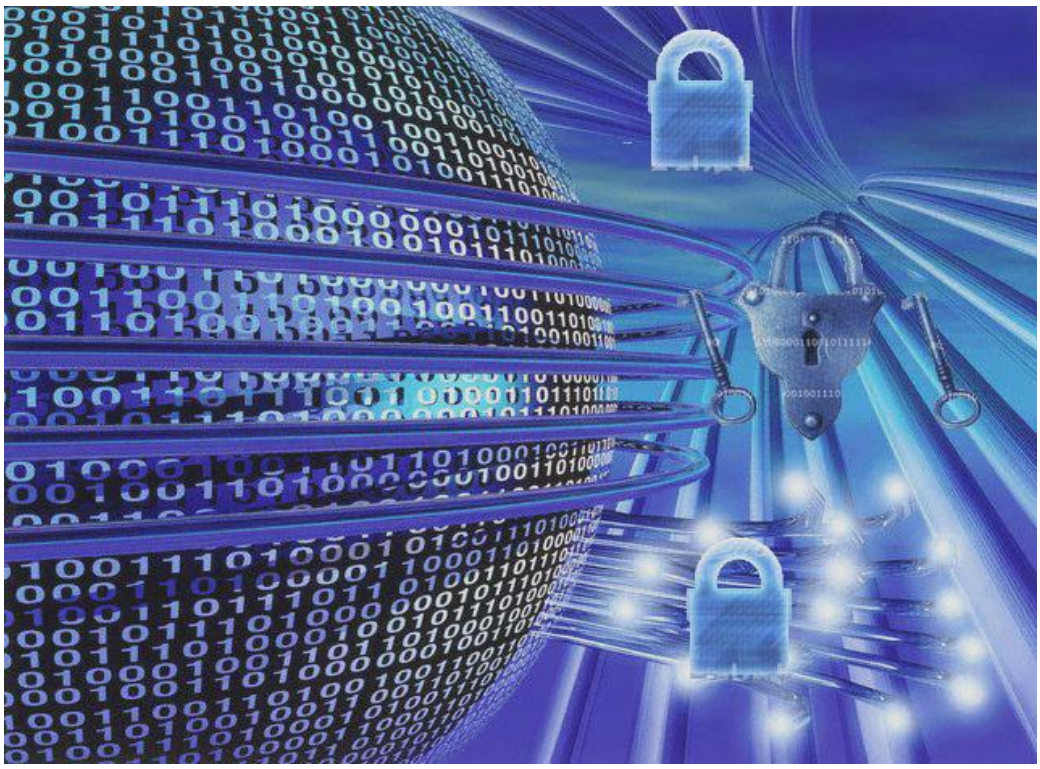
# Segurança Corporativa - Melhores Práticas de Conduta e Conformidade para Colaboradores e Parceiros de Negócios



GMG INTERNET SERVICE

## 1. Introdução

A GMG INTERNET SERVICE LTDA. - alinhada às mais modernas tendências de mercado, de responsabilidade social, sustentabilidade e, sobretudo segurança das informações coletadas e armazenadas em seus sistemas, apresenta sua cartilha **Segurança Corporativa - Melhores Práticas de Conduta e Conformidade para Colaboradores e Parceiros de Negócios**.

Esta cartilha tem como fundamento o Guia de Referência sobre Segurança Corporativa lançado pela Ordem dos Advogados do Brasil, Seção São Paulo em 2015, cujos pilares relacionam-se às questões técnicas que permeiam as atividades dos colaboradores desta instituição, no que tange à segurança da informação, segurança física, patrimonial, monitoramento e auditoria, além de *ECM (Enterprise Content Management/GED)* ou sistema de Gestão de Informações Corporativas.

Incorpora-se, ainda, a este manual, nosso Programa de *Compliance* que tem como princípio basilar a Lei 12.846/2013 que dispõe acerca da responsabilização objetiva da administrativa e civil de pessoas jurídicas pela prática de atos de corrupção contra a administração pública, nacional ou estrangeira.

Todos estes esforços culminarão em um treinamento oferecido a todos os nossos colaboradores para a sua real efetividade, bem como sua previsão em contratos de trabalho de acordo com a legislação trabalhista vigente e a jurisprudência dos Tribunais Superiores sobre temas não previstos na Consolidação das Leis do Trabalho, além de pautar as relações com nossos parceiros, pautadas na justiça e na transparência.

São José do Rio Preto, janeiro de 2017
(revisada em 30 de maio de 2023)

## 2. Objetivo

O objetivo inconteste deste manual é o compartilhamento com nossos colaboradores e parceiros dos valores, princípios e procedimentos, especialmente no que tange a ética, a legalidade e a transparência do nosso negócio.

De forma específica, esperamos:

- Construir um discurso uníssono entre colaboradores e parceiros, de forma a evidenciar nossos valores;
- Consolidarmo-nos no mercado como uma empresa segura, ética e de vanguarda em nosso segmento.

## 3. Quem somos

A **GMG INTERNET SERVICE LTDA.** - é uma empresa sediada na Av. Emilio Trevisan 655, conjunto 303, Bairro Bom Jardim, CEP 15.084-067, na cidade de São José do Rio Preto, estado de São Paulo. Detentora da plataforma e softwares:

**1. Gmg Ambiental** é ecossistema de softwares próprios integrados em uma única plataforma própria e desenvolvida no Brasil pela GMG INTERNET SERVICE LTDA., a Gmg Ambiental é uma plataforma SaaS - Software as a service ou software como um serviço, acesso por login e senha, que roda alicerçada ao software Gomapsgo, que é um sistema de Informações Georreferenciadas - SIG, formato web (em nuvem), com apoio de mapas fornecidos por rede de satélites integrados via API, com objetivo de gerar produtos destinados as seguintes soluções:

**1.1. Monitoramento e Análise de Incêndios**: É um Sistema de monitoramento e georreferenciamento de focos de queimadas e incêndios em propriedades rurais. Funcionalidade: Essa solução permite que toda a área do cliente seja monitorada por meio de satélites. Quando identificamos um foco de incêndio, com a ajuda de algoritmos, determina-se rapidamente as coordenadas do local exato na propriedade. A partir desse momento é enviado um alerta ao cliente, orientando a tomada de decisão para o combate ao fogo;

**1.2. Monitoramento Climático para o Campo**: É uma solução de monitoramento climático referente aos seguintes recursos - "Velocidade e Direção do Vento", "Previsão de temperatura", "Chuva Acumulada Diária", e "Alerta Triplo 30":

"Velocidade e Direção do Vento": Esse recurso entrega muito mais segurança, afinal, ele apresenta a direção e a velocidade do vento. Assim, se houver incêndios em áreas vizinhas, pode-se calcular se existem possibilidades de que ele atinja a área monitorada, auxiliando nas providências que deverão ser tomadas. Vantagens: Maior segurança; e Brigada de Incêndio melhor informada para tomada de decisão.

"Previsão de temperatura": A previsão de temperatura apresenta os dados previstos para o dia seguinte, auxiliando no planejamento diário da safra. Vantagens: Reduz a perda de produtividade; e contribui para a tomada de decisão.

"Chuva Acumulada Diária": O recurso disponibiliza informações referentes à quantidade de chuva dos dias anteriores em milímetros. É possível escolher a data em que se quer acessar a informação, ajudando a compreender os índices de chuva de determinados períodos. Vantagem: Trabalhar de forma estratégica para uma safra produtiva.

"Alerta Triplo 30": O recurso Alerta Triplo 30 é uma tecnologia exclusiva Gmg Ambiental. Ele se organiza tendo como base 3 (três) dados: temperatura, velocidade do vento e umidade. Ou seja, se a temperatura estiver acima de 30º C, a velocidade do vento maior que 30 km/h e a umidade do ar menor que 30%, um alerta será emitido. Sob essas condições, se um incêndio vier a acontecer, ele terá maior probabilidade de difícil combate, oferecendo maiores riscos aos brigadistas. Por isso o alerta de encontro desses três fatores se torna tão importante. Vantagens: Maior segurança; e Brigada de Incêndio melhor informada para tomada de decisão.

**1.3. GMG Relatório Cicatriz**: O relatório cicatriz é uma espécie de dossiê para defesa contra multas ambientais. O relatório apresenta dados referentes ao dia do incêndio, como: temperatura, umidade do ar, como era a probabilidade de risco de fogo, se existia fator triplo 30, em que local o incêndio teve início e como ele chegou na área do cliente. Todas essas informações ajudam a provar que o responsável pelo fogo não foi o proprietário da área. Vantagens: Ajuda na defesa contra processos ambientais; Reduz a chance de multas; Dados climáticos do dia do incêndio; e Rastreabilidade do fogo.

**1.4. GMG Aplicativos para o Campo**: "GMG Gestão de campo" - O aplicativo auxilia na gestão de campo. Ele permite que sejam inseridos, principalmente, dados a respeito de incêndios, mas também sobre polícia, mosca no estábulo, check list de aceiro. O aplicativo é personalizável, ou seja, pode ser adaptado para as necessidades de cada cliente. Vantagens: Agilidade de informação; Conectado com o monitoramento; Alerta do foco por notificação; 100% customizável; Trabalha offline; Imagens do combate ao incêndio; e Painel para baixar relatórios em PDF.

**1.5. GMG Gestão de Focos**: Através da nossa plataforma, é possível extrair relatórios dos focos ocorridos, filtrando por mês, unidade e tipo de preenchimento. Além disso, disponibilizamos um dashboard, onde os gestores de forma rápida conseguem mensurar a assertividade do sistema. Vantagens: Banco de dados com todos os focos que ocorrem nas áreas; Extrair relatórios em gráficos, pdf e excel; e Medir assertividade do sistema através de relatórios.

**2. GomapsGo:** É um Sistema de gestão e informações de landbank e viabilidade; permite demarcar e georreferenciar uma área, permite baseado na demarcação gerar planilhas com viabilidade de negócios, permite baseado na demarcação obter

informações da região como renda per capita dos habitantes, densidade demográfica, estabelecimentos comerciais e outros pontos de interesses, permite criar e cadastrar usuários, gestão dos acessos do usuários, permite criação de pastas para arquivos de conteúdos digitais (PDF, arquivos XML, Vídeos, planilhas);

### 3.1 Organograma

Marcelo Rodrigues Ferraz – CEO - Diretor Executivo

## 4. Prevenção e Segurança Corporativa

O enfoque que será dado a este manual concentra-se em Prevenção. Isto porque, a maioria das fraudes que ocorrem dentro das empresas são descobertas apenas durante os processos de auditoria que constituem-se em processos REATIVOS, isto é, acontecem somente após os desvios terem ocorrido.

Diferentemente também de como pensam grandes instituições que delegam a processos informáticos a redução de suas perdas, entendemos que apenas a implantação destes sistemas não resolve a questão das fraudes empresariais, essencialmente porque a ocorrência de crimes dentro das corporações, incluindo os cibernéticos são realizados por colaboradores de todos os níveis hierárquicos.

**Processos preventivos de segurança sempre devem considerar o fator humano como elemento chave e o mais vulnerável dos recursos corporativos.**

### 4.1 Responsabilidade jurídica das organizações

Além das obrigações trabalhistas e tributárias da organização, de acordo com as leis vigentes no país, há, hoje mais uma questão jurídica que deve ser levada em consideração: o uso dos recursos tecnológicos por seus colaboradores.

Tecnicamente, cabe esclarecer que, de acordo com o art. 935 do Código Civil Brasileiro, a responsabilidade civil é independente da criminal, porém apenas a primeira poderá ser imputada à pessoa jurídica.

Porém nos crimes que envolvem pedofilia e pirataria, utilizando-se de recursos tecnológicos, praticados dentro do ambiente institucional, incorre-se na possível responsabilização do gestor, já que assumiu o risco sabendo da possibilidade do ilícito ocorrer.

Ainda de acordo com o *Código Civil, art. 932:*

*São também responsáveis pela reparação civil:*
*[...]*
*III- o empregador ou comitente, por seus empregados, serviçais e prepostos, no exercício do trabalho que lhes competir ou em razão dele.*

Também a Súmula 341 do Supremo Tribunal Federal, predispõe:

*É presumida a culpa do patrão ou comitente pelo ato culposo do empregado ou preposto.*

No âmbito trabalhista, as organizações ainda devem se preocupar com as consequências da falta de organização, procedimentos e regras de uso de suas tecnologias, porque dentre outros problemas, pode haver incidência de hora extra e questões envolvendo privacidade.

## 4.2 Responsabilidade social e sustentabilidade

As empresas possuem responsabilidades indiretas sobre danos extrapatrimoniais coletivos em termos sociais e ambientais, pois passam a ser considerados agentes transformadores, que exercem elevada influência sobre seus recursos humanos e possuem recursos econômicos e tecnológicos que permitem direcionar seus colaboradores a determinados resultados.

Para melhor esclarecimento, seguem as definições aqui consideradas sobre responsabilidade social e sustentabilidade.

**4.2.1 Responsabilidade Social:** compreende um conceito amplo, segundo o qual as empresas, voluntariamente, integram ações de preocupação social e ambiental nas suas operações e na sua interação com outras partes interessadas.

**4.2.2 Sustentabilidade:** na visão corporativa, trata-se de um novo modelo de gestão dos negócios, em que todos os processos passam a contemplar efetivamente a dimensão social e ambiental, conjugado a boas práticas de governança, esse modelo interage positivamente na dimensão econômica.

Especificamente no caso da GMG, as preocupações que tangem a responsabilidade social e a sustentabilidade são conceitos integrantes dos nossos produtos, uma vez que a prevenção de queimadas é uma das funcionalidades mais importantes do nosso principal software.

## 5. Segurança e proteção

Para maior entendimento, seguem os conceitos de segurança e proteção aqui incorporados.

Segurança: é um conceito intrínseco da necessidade humana, um estado de espírito, já que todas as pessoas carecem de sentir-se seguras em todos os âmbitos de sua vida;

Proteção: é um termo empregado para caracterizar ações planejadas de forma antecipada, para evitar ou reduzir danos causados por agressões contra pessoas, processos, tecnologias e organizações.

No mundo corporativo, segurança representa um estágio atingido de conforto por se implantar ações de proteção, a qual pode ser quantificada tipicamente em baixa, média ou alta, ou ser certificada como adequada, conforme regras e padrões de aceitação internacional, como os propostos na norma ABNT NBR ISO/IEC 27002:2005 (*Code of Practice for Information Security Management*), (ABNT, 2013c) e certificado pela Norma ABNT ISO/IEC 27001:2005 (*Information Security Management Systems – Requirements*), (ABNT, 2013b).

Aceito um determinado nível de segurança, chega-se ao conceito de confiança que pressupões um estado da consciência humana de se considerar seguro.

## 6. Riscos corporativos

Dentro do universo corporativo, os riscos são determinados pela combinação de ameaças, vulnerabilidades e perda dos valores dos ativos, valores esses mensurados com base no impacto dos ativos aos negócios da organização. As perdas podem ser financeiras, materiais, humanas, intelectuais e morais e podem ser valoradas numericamente.

### 6.1 Segurança da informação

Setor responsável pelo cuidado do patrimônio informacional da empresa, alicerçados nos pilares de integridade, confidencialidade e disponibilidade.

### 6.2 Segurança física, patrimonial, monitoramento e auditoria

Entre as ações de segurança corporativa, possuem destaque efetivo todos os aspectos de segurança física, patrimonial, das pessoas, dos processos de monitoramento (CFTV, controle de acesso, autenticação biométrica, *Single Sign-On* SSO S3O, de incêndio e de automação predial e também os processos de gestão de riscos e auditoria interna.

### 6.3 ECM, SPED, IRPJ-e

Outras atividades dentro da empresa que tratam dados em geral, de responsabilidade específica, ECM (*Enterprise Content Management* / GED, ou sistema de Gestão das informações corporativas que, via de regra, são informações digitais ou digitalizadas e armazenadas e tratadas em redes e *Storages* / BIG DATA da organização; os sistemas de comprometimento fiscal e tributário, como o SPED (Sistema público de escrituração digital) e os processos de declarações eletrônicas, como o IRPJ-e que utilizam certificados digitais.

## 7. Fraudes ocupacionais

As fraudes ocupacionais podem ser caracterizadas como aquelas que ocorrem de forma estruturada em diversas áreas da empresa e pouco são divulgadas, em virtude dos enormes escândalos que provocam à instituição.

7.1 Melhores práticas de combate a fraudes ocupacionais

- Certificações antifraudes conferidas por empresas que realizam auditorias internas e externas;
- Elaboração de um Código de Conduta Moral e Ética que possa ser operacional e que seja, de fato implantado;
- Programa de capacitação interna;
- Programa de esclarecimento sobre as mudanças do Código de Ética da empresa;
- Práticas de RH estratégico e seguro.

Por sermos uma empresa pequena, as questões de natureza ética e moral que devem reger a conduta de todos os colaboradores são discutidas em reuniões mensais que abordam este tema e seu impacto na imagem da empresa junto ao mercado.

À medida em que o quadro de funcionários se ampliar, a princípio para dez, estes princípios passarão a integrar um manual escrito que será disponibilizado e discutido entre todos os colaboradores.

## 8. Fraudes cibernéticas

**C**om o advento dos computadores e das redes, as fraudes praticadas contra as instituições tornaram-se mais avançadas e apoiadas por aparatos tecnológicos, como o das redes de computadores que permitem o acesso dos empregados aos dados empresariais de forma legítima, bem como a manipulação dos dados, indevidamente tratados ou perdidos, que podem levar as empresas a grandes perdas e danos irreversíveis.

Com a finalidade de combater fraudes eletrônicas, a auditoria evoluiu, atendendo também a verificação de práticas automatizadas por programas e processos de computadores e redes, denominando-se Auditoria de Sistemas.

A evolução dos dispositivos eletrônicos, telefones celulares, computadores portáteis, entre outros, permitiu o crescimento das fraudes eletrônicas para um patamar denominado Crime Eletrônico.

Crimes Eletrônicos são "os delitos praticados contra ou por intermédio de computadores ou outros dispositivos de informática" (JORGE; WENDT, 2012, p. 18).

Por exemplo, "chupa-cabra" e ou adulteração de *skimming devices*, para burlar Caixas Eletrônicos de Bancos e furtar dinheiro, para adulterar bombas de gasolina, usar telefone celular e GPS para detonar bombas reais, entre outros.

Com a popularização da Internet, novas modalidades de perdas por desvios financeiros configuraram-se, crescendo exponencialmente as fraudes eletrônicas e as cibernéticas, que ocorrem interna ou externamente ao perímetro da organização.

Essas novas práticas de fraudes cometidas com apoio de sistemas e redes, principalmente da Internet, vêm caracterizando os novos cenários dos crimes eletrônicos.

O crime cibernético, caracterizado pelo uso de recursos tecnológicos, pode se materializar provocando consequências bem reais. São exemplos dessa modalidade de delitos: fraudes por intermédio de falsas lojas de comércio eletrônico, crimes contra honra praticados por meio de computadores da empresa, crimes de violação de direito autoral de programa de computador, crime de pornografia infantil, entre outros.

Normalmente o autor de um crime eletrônico praticado contra a empresa não precisa estar no local para desenvolver a conduta criminosa; com o uso de um dispositivo informático conectado à Internet, aquele pode realizar, de qualquer lugar, as ações criminosas intencionadas.

Em geral a imprensa e as mídias de informação têm contribuído muito com a divulgação das novas modalidades de crimes que empregam tecnologias, o que vem favorecendo a conscientização da sociedade.

### 8.1 Crime Cibernético Organizado

Recentemente, foi aprovada a Lei nº 12.850/2013 (BRASIL, 2013c), que definiu a organização criminosa. Segundo o artigo 1º dessa norma legal:

"[...] considera-se organização criminosa a associação de 4 (quatro) ou mais pessoas, estruturalmente ordenada e caracterizada pela divisão de tarefas, ainda que informalmente, com objetivo de obter, direta ou indiretamente, vantagem de qualquer natureza, mediante a prática de infrações penais, cujas penas máximas sejam superiores a 4 (quatro) anos, ou que sejam de caráter transnacional. (BRASIL, 2013c)."

Essa lei também se aplica:

"[...] I - às infrações penais previstas em tratado ou convenção internacional quando, iniciada a execução no País, o resultado tenha ou devesse ter ocorrido no estrangeiro, ou reciprocamente.
[e] II - às organizações terroristas, entendidas como aquelas voltadas para a prática dos atos de terrorismo legalmente definidos. (Redação dada pela lei nº 13.260, de 2016)
(BRASIL, 2013c, Art. 1º, § 2º, incisos I e II)."

Sob esse prisma, ao se defrontar com uma Organização Cibernética Criminosa, é possível fazer alusão às ações delituosas de múltiplas espécies, as quais são praticadas direta ou indiretamente por grupos de pessoas que colaboram entre si para produzi-las através da Internet. A comunidade de *Crackers* (vulgarmente chamados de *Hackers)* atua de forma colaborativa em nível mundial, produzindo programas avançados para favorecer atos criminosos.

Hoje, os produtos de *softwares* (programas de computador) desenvolvidos para explorar vulnerabilidades genéricas ou específicas constituem-se em um verdadeiro Mercado Comercial no submundo da WEB, denominado de *Hacking Prèt-à-Porter*.

Qualquer interessado em atacar organizações ou pessoas, pode comprar, entre tantas ofertas, um *Exploit Zero-Day* e obter resultados garantidos.

Nota-se, também, a utilização da denominada *Deep WEB* como instrumento para a disseminação dos mais variados conteúdos criminosos, principalmente pelo fato dessa plataforma não ser indexada pelos mecanismos de busca, inclusive, em razão dos seus usuários utilizarem navegação anônima, geralmente pelo programa TOR, dificultando a atuação da polícia na investigação de tais delitos.

**8.2 Exemplos de algumas ações do Crime Cibernético Organizado:**

**- *Hacktivismo*:** caraterizado pelo controverso movimento organizado por *Crackers* para a produção de códigos de programas avançados de computador. Essas organizações, muitas vezes, possuem alcance mundial e são formadas por toda espécie de índoles na produção técnica de *Exploits WEB, Trojans, Backdoors*, entre outros vírus. A ideologia pode ser política, social ou religiosa. Como exemplo, o grupo *Anonymous*, o qual ganhou popularidade mundial por seus ataques a *sites* de grandes empresas e governos, inclusive no Brasil.

**- *Scareware:*** criminosos cibernéticos que enganam pessoas, ofertando *downloads* gratuitos de *softwares* (por exemplo, falsos antivírus e utilitários); usam táticas de coerção e outras práticas antiéticas de marketing. Os *softwares* baixados podem ser ineficazes ou, a princípio, podem parecer impedir a ação de certos tipos de vírus antes de infectarem o computador com os seus próprios vírus. Os indivíduos podem, então, ter que pagar aos criminosos para remover os vírus e seus impactos. Às vezes, esses *softwares* não produzem nenhum efeito aparente, mas tornam as máquinas conectadas

na Internet verdadeiras “Zumbis” (máquinas infectadas por *bots* – códigos maliciosos que controlam remotamente as máquinas infectadas) para produção de ataques DoS (*Denial of Service*) e DDoS (*Distributed DoS*), entre outros crimes.

**- *WEB Money Laundering:*** grupos criminosos promovem ações diversas para transformar dinheiro do tráfico de drogas e de outras formas ilícitas em enriquecimento fácil, dinheiro ilegal em dinheiro contabilizado e legalizado perante aos organismos fiscais.

Os golpes de contabilidade forjada são diversos, desde lojas de comércio eletrônico que vendem produtos a custos abaixo do mercado, *sites* de pornografia, *sites* de venda de medicamentos até *sites* de jogos na WEB que faturam e distribuem prêmios. Atualmente, essa prática está ainda mais fácil, pois a criação da moeda virtual (*Bitcoin)* permite a realização de transações financeiras sem a identificação das partes. Os *sites* que vendem produtos e serviços ilegais na *Deep WEB*, como o recentemente fechado *Silk Road* (venda de drogas), utilizam essa nova forma de pagamento.

### 8.3 Ameaças Convencionais

No gênero de fraudes cibernéticas, encontra-se o uso de alguns termos genéricos, tendo em vista que esses já se tornaram comuns para a sociedade brasileira pelo grande número de ocorrências e pelos impactos de todos os níveis divulgados pelas Mídias Informativas. Entre eles, como exemplos de desdobramento e evolução, tem-se o que segue:

**- Ataques de Vírus:** muitas organizações, nos últimos 20 anos, experimentaram prejuízos de diversas espécies com o ingresso de Vírus, *Worms*, *Trojans*, *Rootkits*, *Spywares*, *Adwares*, *Malware*, entre tantas outras ameaças que exploram as vulnerabilidades de sistemas desprotegidos ou desatualizados e a privacidade em geral, bem como exploram a ingenuidade ou o descuido dos usuários. Todos esses termos, para designar espécies de ataques do mundo digital, fazem parte do cotidiano corporativo, sendo amplamente combatidos por diversas ferramentas de *softwares* (programas de computador). Esses ataques representam ameaças reais e passam a ser elementos de base para ataques mais avançados; por isso, devem ser devidamente valorizados e tratados.

**- Ataques do Tipo *Phishing:*** o *Phishing Scan* é uma das grandes preocupações corporativas quanto aos crimes cometidos com o uso da Internet. Baseia-se no envio de uma mensagem (via *e-mail*, *Twitter, Facebook, SMS* etc.), com o objetivo de explorar a ingenuidade dos internautas e obter códigos de acesso, dados financeiros, informações pessoais e familiares, buscando furto de identidade, preferências pessoais, entre outras informações.

As situações de *Phishing* mais impactantes envolvem o envio de *e-mail* que, ao invés de conter *links* que direcionam para um formulário, no qual é requerida informação que se almeja, são redirecionados às páginas fraudulentas da WEB que contêm programas maliciosos (vírus, *Trojans*), os quais se instalam automaticamente e replicam-se no computador da vítima, contaminando arquivos que podem ser repassados a terceiros como um vírus.

Esses programas pertencem, muitas vezes, à classe dos *Key/Screen Loggers Vírus* e podem registar a sequência de teclas pressionadas, as telas visitadas ou as atividades

realizadas, inclusive a movimentação do cursor e/ou do *mouse*. Esses programas, depois de recolherem as informações, enviam-nas pela Internet para um *site* controlado pelo perpetrador da fraude, que faz uso comercial delas.

Na legislação brasileira, o *Phishing,* quando utilizado para a apropriação de dados bancários da vítima para o posterior saque, configura o crime de furto qualificado mediante fraude (BRASIL, 1940, Art. 155, § 4o), com pena de 2 a 8 anos de prisão e multa.

De forma simples, o furto de identidade, geralmente, é cometido por intermédio de técnicas de *Phishing Scan*, que se vale da ingenuidade dos usuários de computadores, através de técnicas de engenharia social avançada, e buscam obter dados pessoais diversos que possam individualizar perfis que permitam aos criminosos usarem o nome e os dados das vítimas para se caracterizar efetivamente como elas e cometerem atos ilícitos através da Internet.

**- Ataques para *Hoax* / Boato:** *Hoax*, em tradução quase literal, é um embuste. Na prática, consiste em uma mensagem de *e-mail* com conteúdo alarmante e mentiroso que tem evoluído para casos muito mais graves e práticas de *Bullying WEB*. De certa forma, utilizam a boa fé das pessoas para propagarem boatos e, assim, tornarem-se "uma atraente verdade". Um bom exemplo de um *Hoax* são as mensagens que habitualmente circulam pelos *e-mails*, em que dizem sobre um novo vírus, um novo ataque ou cuidados que devem ser tomados, e pedem para passar ou retransmitir a mensagem. Há, também, o exemplo de correntes: "Envie esta mensagem para 15 pessoas e ganhará dinheiro (ou outro bem)". Na verdade, ganhará mesmo é um susto.

**- *Spam:*** inicialmente, referia-se ao envio não autorizado de *e-mail* com conteúdo comercial. Atualmente, o *Spam* pode ter até mesmo conteúdo eleitoral, sendo disseminado em outras formas de comunicação eletrônica, como, por exemplo, redes sociais, SMS e aplicativos de comunicação instantânea. A legislação brasileira não proíbe a prática do *Spam* comercial. Na verdade, o Superior Tribunal de Justiça (BRASIL, 2009) entendeu que o *Spam* é um mero aborrecimento, e não viola a privacidade do destinatário. Contudo, na propaganda eleitoral, o candidato só poderá enviar mensagens para eleitores previamente cadastrados gratuitamente (BRASIL, 1997, Art. 57-b, III).

Na prática, é possível observar que os crimes cibernéticos produzidos através de ameaças convencionais seguem sempre a exploração das vulnerabilidades do elo mais fraco, o usuário, que nas organizações são elementos-chave para o alcance dos objetivos estratégicos.

### 8.4 Ameaças Persistentes Avançadas (APA)

Nos últimos anos, observa-se um grande avanço e maior sofisticação nas técnicas de ataques, os quais, seus autores, passaram a trabalhar cada vez mais em ações criminosas e até em guerra cibernética.

Os grandes alvos de ataques na WEB foram os *sites* de organizações e organismos de governos de diversos países, como amplamente divulgado pelas mídias informativas no mundo todo, sendo alvo dos ataques: hospitais, bancos e empresas de todos os portes e em diversos setores de atividades. Os ataques sempre objetivam furtar dados e informações sensíveis, as quais podem ser comercializadas ou empregadas para diversas práticas de chantagem, extorsão e ganhos financeiros.

No processo evolutivo dos ataques, os criminosos criaram ferramentas aprimoradas que invadem as Redes Corporativas, escondem os rastros, produzem autodefesa contra as proteções de *Firewalls* e produtos de segurança, escondem-se e permanecem em hibernação até o momento de conseguirem obter o que eles desejam.

Hoje, os ataques caracterizam-se por ameaças de persistência nas organizações-alvo, ou seja, se a sua empresa é alvo, já pode ter sido invadida por APA (Ameaça Persistente Avançada). Os principais alvos são os empresários e colaboradores de nível de Diretoria e Gerencial, os quais, legitimamente, possuem senhas com direito de efetuar pagamentos, movimentar fortunas e acessar dados de planos estratégicos e de P&D.

Alguns exemplos do que ocorre no mundo através de APA:

**- *Customer Data Loss:*** furto de dados de cadastro de clientes, principalmente de empresas financeiras, empresas de serviços médicos, entre outras. São realizadas por ataques especializados as Redes Corporativas em que sua maioria, não deixa rastros ou interferirem em nada, passando totalmente despercebidos dos técnicos da empresa lesada. As informações obtidas são analisadas e comercializadas para facções do crime organizado, que as usam para extorsão, chantagens e comércio.

**- *Intellectual Property Theft***: caracteriza-se por invasões veladas, de identificação pouco provável, da mesma forma que ocorre com *Costumer Data Loss*, através da qual criminosos por vezes patrocinados por organizações concorrentes ou nações, objetivam localizar e furtar ideias, projetos, especificações de produtos, segredos comerciais, informações do processo ou metodologias, que podem ser de grande valor, podendo produzir vantagem competitiva ou até mesmo vantagem operacional ou tecnológica. Essa modalidade pode ser considerada a evolução da clássica Espionagem Industrial.

***Theft From Business:*** furto financeiro de empresas passou a ser uma epidemia mundial, e vem ocorrendo através de técnicas APA do Crime Cibernético Organizado. O uso de invasões veladas às redes corporativas tem permitido, quase sempre com a colaboração de um ou mais *insider* (informantes internos), a realização do pagamento de títulos e transferências financeiras fraudulentas, lesando de imediato o caixa das empresas. No Brasil, a adulteração de boletos bancários com a indicação de dados de novo cedente cresce nas notícias policiais.

***Fiscal Fraud:*** usando os mesmos recursos e artifícios das ações de *Theft From Business*, os criminosos utilizam os acessos corporativos para desviar pagamentos legítimos de impostos para contas particulares, lesando a empresa e o governo. A empresa, em grande parte, só fica sabendo quando algum gestor não envolvido no esquema da fraude recebe aviso, cobrança ou a visita da fiscalização.

***Theft From Business Extortion:*** esse golpe tem sido crescente, posto que, após a APA ter sido consolidada, o atacante mantém domínio total sobre as bases de dados e a infraestrutura de tecnologia da organização-alvo. A partir desse ponto, o processo de extorsão ocorre através da solicitação de dinheiro em espécie para liberar os acessos, caso contrário, a organização arcará com as consequências, tais como: o redirecionamento de seus *links* comerciais para *sites* de pornografia, a criptografia de dados, entre outras ameaças que exploram o tempo de recuperação e a idoneidade da imagem corporativa.

**- Alerta**: os ataques do tipo APA normalmente duram meses, e até anos, antes de se tornarem lesivos.

### 8.5 Entendendo Fraudes Cibernéticas

Fraude Cibernética, no âmbito empresarial e corporativo, é toda tentativa ilícita de acesso ou obtenção de dados empresariais, corporativos e de organismos de governo, cometida através da Internet. Também podem ser denominadas de Crimes Cibernéticos.

As fraudes cibernéticas tornaram-se uma verdadeira epidemia que causa consequências aterrorizantes dentro dos ambientes empresariais, principalmente pelo desconhecimento tecnológico aprofundado dos gestores, e pelos riscos efetivos que oferecem aos sistemas e às bases de dados sensíveis. Portanto, se o corpo administrativo da diretoria e da alta gerência não estiver atento em combatê-las, aqueles, categoricamente, podem colocar a organização em situação de insolvência.

Hoje, de alguma forma, todas as organizações estão expostas às fraudes, sejam cibernéticas ou não. Os melhores e mais sofisticados ambientes organizacionais, inclusive os mais controlados, podem ter falhas desconhecidas, exploradas de forma integrada por seus colaboradores legítimos e em parceria com o crime organizado internacional.

A comunidade científica e pesquisadores sabem claramente que boa parte das fraudes cibernéticas é materializada através da exploração do "elo mais frágil", ou seja, da ingenuidade do usuário. Logo, grande parte do sucesso efetivo do crime cibernético está associada à conivência, direta ou indireta (direta pela participação ativa e indireta pela displicência às regras), dos empregados ou dos próprios usuários da Internet.

Por exemplo, a evolução das tecnologias tem simplificado o uso de recursos computacionais e das redes a todos os cidadãos do mundo civilizado. Essa revolução das tecnologias, por outro lado, também promove novas oportunidades de usos, costumes e modalidades de crimes sociais. Estamos no Século 21, terceiro milénio, e a mobilidade da comunicação pessoal e corporativa está crescendo de maneira desordenada, através de *smartphones, tablets*, *ultrabooks* e outros dispositivos móveis empregados em todas as classes sociais. Esse fato pode representar um dos maiores riscos da atualidade quanto às fraudes cibernéticas.

### 8.6 Consumerização, BYOT (BYOD, BYOA), BYOW

A consumerização das tecnologias deve ser entendida como um movimento das grandes indústrias mundiais na busca da redução de custos, pois a estratégia anterior estabelecia duas linhas de produção: Produtos *Low End* – para consumidores em geral do mercado, e Produtos *High End* – para usuários empresariais ou para empresas, normalmente com características mais avançadas. A atual estratégia de redução de custos é uniformizar os produtos, como telefones celulares, *smartphones*, *tablets*, *notebooks* e *ultrabooks*, a fim de que todos sejam da linha *High End* (alta tecnologia), atendendo, assim, consumidores comuns e empresas.

Como resultado da consumerização, os equipamentos com características mais avançadas ficaram mais baratos e disponíveis para aquisição por grande parte dos consumidores. Essa questão levou os consumidores domésticos, cuja população economicamente ativa também trabalha em empresas, a querer utilizar os seus equipamentos pessoais no ambiente empresarial, tendo em vista que, por vezes, seus equipamentos possuíam características de desempenho melhores que a dos equipamentos ofertados pelas organizações. A pressão dos empregados em usufruir de

seus próprios equipamentos promoveu uma revolução de aceitação pelas empresas, denominada BYOD – acrônimo em inglês de *Bring Your Own Device* – ou seja, traga seu próprio dispositivo.

A prática desenfreada do BYOD nas organizações, o qual aglomera o BYOP – *Bring Your Own Phone* (traga seu próprio celular) e o BYOPC – *Bring Your Own PC* (traga seu próprio computador pessoal), acabou por disseminar as práticas mais exóticas de BYOT – *Bring Your Own Technology* (traga sua própria tecnologia) que, por consequência, englobou também a BYOA – *Bring Your Own Access and Application* (traga seu próprio acesso e programas). O BYOT é vetor de Tecnologia Disruptiva que vem causando, e ainda vai causar muito transtorno às organizações, por questões de gestão legais, mas, essencialmente, pelas vulnerabilidades e pelo baixo nível de proteção existente para todos os equipamentos móveis. É importante compreender que as fragilidades do BYOT/BYOD, principalmente pelas redes de alta velocidade 4G e 5G, serão amplamente exploradas pelo crime organizado e produzirão muitas Fraudes Cibernéticas.

Ainda assim, ao optar por esse modelo, as organizações devem ficar atentas, devem conhecer para assumir o risco e, acima de tudo, ter uma previsão no contrato de trabalho dos funcionários, envolvendo cláusulas específicas ou, pelo menos, uma referência à determinada norma interna específica para o respectivo cenário.

## 8.7 Melhores práticas e recomendações de defesa

As ações de defesa contra as Fraudes Cibernéticas ou Crimes Cibernéticos podem ser planejadas e implantadas de inúmeras formas, e com alcance de efetividade. O importante é ter consciência da necessidade urgente de proteger, de forma concreta, dados sensíveis no ambiente empresarial, independente dos dispositivos que irão acessá-los.

Para que haja uma compreensão executiva, para profissionais não técnicos, abordam-se, a seguir, sucintamente, as melhores práticas ou recomendações para o sucesso no combate às fraudes cibernéticas.

Nunca esqueça que, no ambiente virtual ou espaço cibernético, os riscos são reais e trazem consequências no âmbito presencial.

Tenha em mente que o alvo dos criminosos virtuais sempre será explorar as vulnerabilidades tecnológicas e humanas que possam permitir o acesso aos dados sensíveis empresariais (por exemplo, senhas de acesso) e também pessoais.

Esteja sempre atento ao utilizar redes que permitam acesso à Internet, observando, basicamente, as hipóteses de ações criminosas descritas a seguir.

### 8.7.1 Engenharia Social

Técnicas de exploração da ingenuidade do usuário, que usualmente estão focadas no senso de urgência, de responsabilidade ou de curiosidade, atraindo a atenção das vítimas, oferecendo, por exemplo: grandes ofertas por tempo limitado ou obtenção de fotos sobre um acidente. As promoções falsas e o interesse em obter informações podem levar as pessoas a clicarem em *hiperlinks* que instalam automaticamente programas maliciosos, os quais produzirão a obtenção das informações sensíveis, ou outros estragos de contaminação e prejuízos à empresa e aos usuários. Um dos maiores instrumentos da Engenharia Social é o *Phishing Scan* através de *e-mails* e do redirecionamento a *hiperlinks* para *sites* contendo *malwares*.

**8.7.1.1 Como se defender**:

Esteja atento, sempre desconfie e não acredite no que esteja lendo, mesmo que o remetente seja confiável;

Não clique em *hiperlinks* que receber através de *e-mails*;

Procure nos mecanismos de buscas outras referências sobre temas ou indicações recebidas por *e-mail*; nunca confie imediatamente;

Tenha em seu PC um bom antivírus atualizado e um *Personal Firewall* de reputação, devidamente configurado.

**8.7.2 Resultados de Busca Infectados**

Ataques conhecidos como *Blackhat SEO*, são produzidos por *crackers* que manipulam as ferramentas de busca, fraudando-as com o objetivo de que os *links* para *sites* maliciosos sejam os primeiros na lista de resultados. Esses *links* levam as vítimas para páginas que possuem mecanismos exploradores e infectam o computador, a fim de roubar informações financeiras e, na maioria dos casos, a identidade das próprias vítimas.

**8.7.2.1 Como se defender:**

Esteja atento, sempre desconfie e não acredite fielmente nos resultados de buscas, principalmente quando estiver procurando temas de grande procura popular e encontrar um *site* novo ou estranho em primeiro lugar; quando encontrar um site suspeito em primeiro lugar, antes de clicar no *link*, busque novamente referências em outros buscadores sobre o nome do *site*, e só entre no mesmo após ter convicção de que é legitimo e seguro. No entanto, o risco sempre existirá;

Uma alternativa que está crescendo em confiabilidade é consultar a *URL Blacklist* ou utilizar serviços de checagem de sites como o *Google Safe Browsing* (Navegação Segura) ou, como exemplo, WOT (*WEB of trust*): <http://secureurlchecker. appspot.com/> e *Sucuri Site Check* <http://sitecheck.sucuri.net/scanner/>, antes de entrar no site pesquisado;

Pratique a prevenção; é melhor prevenir do que ter sérios problemas financeiros, jurídicos, e que possam afetar sua reputação.

**8.7.3 Fraudes nas Redes Sociais**

Esse crime vem crescendo através de mensagens postadas automaticamente no perfil da vítima, por amigos descuidados que tiveram suas contas comprometidas (invadidas) ou mediante recados particulares que pareçam estranhos, e a levará, com frequência, a acessar *sites* maliciosos ou a *malwares*, com objetivos de ganhos financeiros. O crescimento das redes e plataformas populares, como *Facebook, Twitter*, *Skype*, dentre outros, tem trazido esse tipo de ameaça, que está cada vez mais sofisticada e comum. Como exemplo, temos o poderoso vírus multiplataforma *Koobface*, cuja especialidade é atacar as redes sociais.

**8.7.3.1 Como se defender:**

Esteja atento, sempre desconfie e não acredite fielmente em tudo que vivencia nas redes sociais;

Procure trocar suas senhas periodicamente e manter suas configurações de privacidade ativas, sempre publicando informações discretas, sem muitos detalhes ou fotos que permitam sua integral identificação, localização e furto da sua identidade (dados que permitam que alguém se passe por você);

Muita atenção com os *links*, todo cuidado é pouco ao clicar em *links* recebidos de amigos e desconhecidos, pois podem ser falsos e causar arrependimento. Sempre descarte *links* que peçam para instalar alguma aplicação para executar um filme ou que o levem a abrir arquivos executáveis ".exe". Quando houver dúvida, recuse. Caso tenha sido enviado por um amigo, confirme com ele verbalmente antes de acessar. Se for de alguma empresa, abra outra janela do navegador e busque verificar se a URL é segura ou oficial, para não cair em golpes de sites clonados.

Se você não for formalmente autorizado a falar em nome da sua empresa, não faça comentários ou divulgue informações da organização, por mais
simples que pareçam, em redes sociais. Assim, é possível evitar vazamentos de informações sensíveis e comprometimentos legais.

### 8.7.4 Assédio moral e sexual através dos recursos da empresa ou do BYOT

Crescem os casos de assédio moral e sexual com o uso de *e-mails*, SMS, JSMS e outros, através dos equipamentos de Mobilidade Corporativa, primordialmente, em empresas que não implantaram adequadamente - a grande maioria - as melhores práticas para a adoção do BYOT. É sabido que esse tipo de ação pode acarretar responsabilidade jurídica para a empresa e para o autor, seja na esfera cível ou na trabalhista.

#### 8.7.4.1 Como se defender:

Esteja atento, sempre desconfie e não dê crédito a qualquer mensagem recebida por serviços de *e-mail*, SMS, JavaSMS e outros, que receber no seu smartphone, por mais absurda que sejam as mensagens. Os remetentes valem-se da falta de controle das organizações e acham-se anônimos e impunes quando usam seus próprios equipamentos;

Quando receber uma mensagem que contenha assédio (humilhações, afrontas, comentários constrangedores, rebaixamento, xingamentos, calúnias vexatórias, coação, convites multiafetivos, tentativas de chantagem etc.), nunca apague as mensagens ou e-mails, preserve-os como prova judicial, pois o arquivo é o documento original;

Use efetivamente os *e-mails* e *Short Messages*, que promovam assédio de qualquer natureza, para penalizar os responsáveis, pois mesmo remetentes sem identificação ou com identificação fraudulenta podem ser localizados através de investigação pericial. Denuncie o seu caso para os responsáveis pela Segurança Corporativa da sua organização e, quando envolver ilícitos penais, denuncie também para os organismos policiais ou organizações específicas para denúncia;

Para a organização, esteja atenta às leis aplicáveis em relação ao monitoramento e ao uso das informações coletadas como prova judicial. Nunca monitore sem prévia ciência do colaborador.

**Denuncie!** Existem dispositivos próprios para receber sua denúncia; por exemplo, <http:// www.safernet.org.br/site/denunciar>.

Delegacias Policiais sobre Cibercrimes no Brasil:

http://www.safernet.org.br/site/prevencao/orientacao/delegacias

## 9. Prevenção e precaução

Para o enfrentamento dos crimes que assolam as empresas e corporações, faz-se necessário o estabelecimento de estratégias de proteção que, se devidamente implantadas, possam amenizar os riscos e os impactos, caso algum evento criminoso venha a ocorrer. As estratégias de proteção devem se valer dos princípios da Prevenção e da Precaução para alcançar os resultados esperados:

**Prevenção:** entendem-se as ações que podem minimizar os efeitos sobre os danos previstos, pois há "certeza científica" sobre o dano que determinados eventos podem causar. Portanto, os riscos são conhecidos.

**Precaução:** entendem-se as ações de menor efeito, que podem ser previstas devido à "incerteza científica" dos danos e dos impactos da ocorrência de determinados eventos, pois a cláusula *in dúbio* leva a entender dessa forma, portanto, nesse caso, os riscos não estão perfeitamente identificados.

O tema Prevenção e Precaução trata-se de um conjunto de ações recomendadas por especialistas, que objetivam ampliar o nível de segurança e estabelecer um processo de confiança ajustado às expectativas das organizações modernas.

As grandes ações de Prevenção e Precaução podem ser genericamente identificadas conforme descritas na sequência.

### 9.1 Prevenção Organizacional

Ações ligadas a Prevenção Organizacional compreendem o planejamento da implantação de processos e estruturas organizacionais preparadas para atender a demandas de riscos que podem ou tendem a ocorrer. Ressalta-se que, nesse cenário, a interação das áreas torna-se essencial. Entre as principais ações de Prevenção Organizacional, destacam-se as citadas a seguir:

**- Organização Segura de Recursos Humanos**

Consiste na reformulação de processos na área de Recursos Humanos, dando ênfase aos critérios de Recrutamento e Seleção de colaboradores, com base em uma avaliação criteriosa dos candidatos em termos de preceitos morais, avaliação da capacidade de cumprir leis, regras e regulamentos, avaliação de antecedentes pessoais e familiares, entre outras técnicas de avaliação da índole, atentando-se para que não optem por requisitos que possam caracterizar discriminação. Além disso, a segurança jurídica de seus documentos, desde a contratação e o acesso às Políticas e Normas, bem como em termos de ciência e responsabilidade, quando aplicáveis.

**- Escritório de Segurança Corporativa**

Envolve o estabelecimento de uma pequena estrutura organizacional específica e voltada para a Segurança Empresarial ou Corporativa, sendo um setor isento e totalmente desconectado das demais áreas da organização. Esse Escritório de Segurança deve se reportar ao mais alto escalão da organização, preferencialmente ao

CEO ou ao Presidente do Conselho de Administração. Compete ao escritório definir as Regras de Segurança da Organização, auditar a implantação e efetuar a Governança da Segurança.

O Escritório de Segurança nunca deverá se subordinar à área de TIC (Tecnologia da Informação e Comunicação), pois a área de TIC tem a missão de implantar e operar Processos de Segurança da Informação (SI), e não de defini-los e auditá-los, embora seja comum nas empresas de menor porte a ausência dessa equipe, de forma que a TI acaba por assumir toda a responsabilidade por Segurança da Informação. Na prática, as empresas devem ser flexíveis. O cenário ideal exige o Escritório de Segurança Corporativa; no entanto, caso esse venha a assumir SI, certamente deverá ter em sua equipe profissionais da área de tecnologia.

**- Política de Prevenção e Segurança Corporativa**

Compreende uma nova visão no desenvolvimento das Políticas de Segurança, das quais processos de Prevenção e de Precaução devem ser destacados. As organizações mais evoluídas necessitam promover programas preventivos contra as fraudes e transformar essa iniciativa em vantagem competitiva. A implantação de um serviço de Delação Segura que seja isento, terceirizado, de preferência, que mantenha uma ouvidoria séria para obter informações sobre eventuais suspeitas a colaboradores, passa a ser fator determinante nas mais avançadas Políticas de Prevenção e Segurança das organizações de sucesso do Século 21.

Além disso, as Políticas e Normas devem, preferencialmente, atender não apenas as normas internacionais, mas também a legislação nacional aplicável, sendo essencial a integração direta com um serviço jurídico especializado.

## 9.2 Prevenção Jurídica

Ações ligadas a Prevenção Jurídica compreendem ao planejamento de implantação de processos e instrumentos preventivos, preparados para atender a demandas de riscos que, podem ou tendem, a ocorrer na organização, envolvendo direta ou indiretamente a esfera judicial. Dessa feita, a interação das áreas de RH (Recursos Humanos), TI (Tecnologia da Informação), bem como Infraestrutura e Segurança Corporativa, devem interagir diretamente com um serviço jurídico especializado. Entre as principais ações de Prevenção Jurídica, é possível destacar as que seguem.

**- Contratos, Termos de Aceitação e Normas**

Para que uma organização possa ampliar seus processos preventivos em termos de segurança, muitos instrumentos de relacionamento multilaterais, como contratos, por exemplo, devem endereçar cláusulas de confidencialidade, de uso seguro de informações privilegiadas, de uso responsável de recursos tecnológicos, de uso de imagem, de propriedade intelectual, entre tantas outras. Apenas através da prevenção jurídica, alinhada ao Direito Digital, será possível alcançar um nível de segurança adequado.

No âmbito de prevenção jurídica, acaba por ser primordial a elaboração de regras claras. Justamente por possuir responsabilidade objetiva pelos atos de seus empregados, o empregador deve agir com diligência e precaução, fazendo valer seu poder diretivo, fiscalizador e punitivo.

Quando se trata de relação empregatícia, as exigências atuais de proteção, tanto

da organização quanto dos colaboradores, exigem um perfeito entendimento “do que pode e do que não pode” ser feito, utilizado, divulgado, acessado, entre outras regras. Portanto, instrumentos de Acordos, Termos de Ciência, Termos de Responsabilidade, Normas Internas, Procedimentos Técnicos, Procedimentos Operacionais e outros deverão, necessariamente, possuir aval jurídico que busque garantias preventivas nas relações, sejam com empregados, parceiros, fornecedores, clientes ou acionistas.

**- Códigos de Conduta e CRS**

As organizações estão vivenciando a necessidade de garantir ao mercado a sua preocupação quanto à conduta moral, ética, à responsabilidade social e à sustentabilidade, especificadas através de instrumentos como Códigos de Conduta ou Códigos de Responsabilidade Social Corporativa (CRS).

Para efeitos de prevenção jurídica, principalmente no âmbito da Justiça do Trabalho, não basta que existam as regras, mas essas devem ser entregues de forma clara e comprovadamente disponibilizadas em local de fácil acesso, seja por uma intranet ou entrega impressa, entre outros meios.

Sendo assim, o código de conduta, além de tratar das questões éticas, acaba por ser uma forma mais prática de interação e exposição dos principais aspectos das Políticas e Normas Internas.

Ainda do ponto de vista da prevenção jurídica, seria conveniente que esses instrumentos fossem construídos de forma a permitir que a operação de gestão e a direção empresarial avaliem o quanto os preceitos estabelecidos estão sendo cumpridos pelos colaboradores, a fim de que haja uma perfeita transparência quanto à Determinação Executiva expressa nesses instrumentos e ao seu efetivo cumprimento. A possibilidade de mensurar efetivamente a adesão e as práticas dos colaboradores, assim como tomar medidas corretivas caso haja desvios, passa a ser fundamental para o sucesso dos negócios.

Por envolver questões técnicas que acabam por exigir conhecimentos de tecnologia e até mesmo de termos, recursos, processos e funcionalidades, muitas empresas optam por terceirizar o serviço jurídico relacionado às questões tecnológicas para escritórios especializados, ainda que tenham um departamento jurídico interno, mas esse não atua diretamente nessa área.

Cuidados para obtenção de provas, acompanhamento de perícias e, até mesmo, a participação em reuniões estratégicas da corporação, ou empresa, acabam por fazer parte do cotidiano do advogado especializado. Além disso, é preciso extrema atenção sobre casos concretos por intermédio de jurisprudências, julgados recentes e vigência de novas leis.

### 9.3 Prevenção Tecnológica

Ações de Prevenção Tecnológica devem ser consideradas quando for possível os crimes ocorrerem através de Redes de Computadores da Internet, com o acesso indevido a sistemas de informação, e tantos outros aspectos envolvendo tecnologias. Na prática, todo o investimento que as organizações fazem em sistemas e processos de Segurança Corporativa da Informação enquadram-se na classe de prevenção. Aborda-se esse tema, tendo em vista que algumas ações fundamentais são comumente negligenciadas e tornam as prevenções existentes totalmente ineficazes para punir os criminosos. Para garantir o investimento em segurança aplicada em tecnologias, são necessárias atitudes específicas, como as citadas a seguir:

**- Preservação de Provas Eletrônicas**

De forma geral, os sistemas eletrônicos são responsáveis por mais de 90% do registro de evidências que podem ser empregadas para localizar e desvendar fraudes ocupacionais, ou seja, aquelas cometidas por colaboradores, utilizando os recursos computacionais das organizações. Ocorre que, por falta de informação, acompanhamento jurídico e/ou capacitação dos técnicos de TIC, essas evidências não são tratadas adequadamente e são adulteradas ou perdidas, deixando de atender aos requisitos legais para serem utilizadas em juízo. A grande recomendação de prevenção é a preservação das provas eletrônicas para que essas, realmente, constituam-se em instrumentos concretos para servir às empresas. O correto, apesar de custoso, é desligar, retirar e substituir o computador de um colaborador quando houver suspeita de indícios de fraudes. A máquina suspeita deverá ser examinada por técnicos qualificados para buscar as evidências técnicas da possibilidade de fraude. No entanto, cuidado! Até mesmo para desligar o computador deve-se observar algumas premissas. Em alguns casos, essa ação também poderá afetar diretamente as provas.

Deve, sim, existir um procedimento efetivo, porém, dependendo do caso, o procedimento deve ser reavaliado, e caberá à empresa, com embasamento técnico e legal, decidir o que melhor lhe convier.

Os tribunais brasileiros reconhecem a validade jurídica dos *logs* e do número de IP, que justamente identifica o computador que realizou o acesso a determinado endereço da Internet (BRASIL, 2011b).

Dessa forma, mesmo não havendo obrigação legal, é fundamental que as empresas armazenem os seus *logs*. A norma *PCI Data Security Standard*, por exemplo, recomenda a sua guarda por, ao menos, um ano.

**- Perícia Forense Computacional**

As organizações mais avançadas já se deram conta de que vale a pena investir na qualificação de colaboradores dos escritórios de Segurança, para que esses possam examinar máquinas e outros elementos de rede suspeitos, através de processos periciais computacionais, com o fito de encontrarem as evidências de fraudes, desvios de conduta e até mesmo de crimes cometidos com recursos da organização. Os técnicos capacitados aprendem a preservar as evidências, de forma que elas possam ser utilizadas judicialmente, fornecendo instrumento seguro para que a área jurídica possa empregá-las, a fim de desvendar e solver tentativas ou existências de crimes internos e externos. Os processos de Perícia Forense Computacional Corporativa garantem que as evidências coletadas sejam aceitas nos tribunais. Por outro lado, organizações de menor porte possuem a opção de contratar empresas especializadas para o trabalho de perícia quando necessário.

## 9.4 Prevenção de Inteligência e Contrainteligência

No presente momento, o mercado e a globalização da economia tornaram as empresas altamente competitivas e, inclusive, vorazes contra a concorrência. É muito comum observar organizações avançadas investindo em Departamentos de Inteligência Competitiva para entenderem seu posicionamento no mercado, e as ações e inciativas dos concorrentes. Da mesma forma, tem-se observado o crescimento da concorrência

desleal, crime previsto na Lei de Propriedade Industrial. Por exemplo, cita-se a "Infiltração" que coloca efetivamente um "agente" contratado pelo concorrente a trabalhar na organização a ser lesada, para obter, legitimamente, informações privilegiadas e transmiti-las aos interessados. Estando, pois, as organizações conscientes disso, estão investindo em instrumentos e processos preventivos, não só para localizar esses possíveis agentes, mas para combater o vazamento de informações. Muitas, inclusive, já estão atuando em contrainteligência, divulgando aos agentes informações tratadas para ludibriar a concorrência.

A prevenção de vazamento de informações vem sendo tratada nas Redes Corporativas mediante os softwares denominados DLP (*Data Loss Prevention*) que bloqueiam, através de regras, a remessa de dados pelas redes e determinam o indício de vazamentos, colocando sob suspeita ou sob análise mais apurada os prováveis informantes. As áreas de segurança nas organizações devem ser capacitadas para efetuar investigação interna e apurarem vestígios e evidências que possam constituir cenários de crimes internos de vazamento de informações estratégicas e sensíveis.

**- Prevenção é a melhor defesa das organizações.**

## 10. RECOMENDAÇÕES PARA SEGURANÇA CORPORATIVA

### 10.1 Conselho de Administração

A intervenção na administração das organizações acontece por intermédio dos cargos de administradores designados, sócios, membros de Conselho Consultivo, Administrativo e/ou Fiscal, sempre na dependência da necessidade e do perfil empresarial.

Os Conselhos de Administração são mandatórios em empresas de capital aberto, mas suas práticas não são exclusivas a elas, pois muitas sociedades limitadas estão aderindo às regras da sociedade anônima, objetivando a profissionalização da forma de gestão.

O certo é que não seja vedado às Sociedades Limitadas constituírem sua administração por meio de Diretorias Executivas e Conselhos Consultivos ou de Administração, cuja composição seja distinta, ou seja, diferente daquela formada pelo quadro societário. Essa prerrogativa está alinhada às melhores práticas de Governança Empresarial, no entanto, imputam diretamente responsabilidades aos Conselhos (consultivo, administrativo, fiscal).

Na prática, nas sociedades limitadas, sócios e administradores delegam ao Conselho Consultivo a análise de algumas questões estratégicas, como a Segurança Empresarial, ou seja, nas grandes corporações ou até na média e pequena empresa, os Conselhos podem ser estabelecidos e devem possuir atribuições estratégicas de analisar e recomendar ações efetivas na busca da melhoria do desempenho, da segurança e da continuidade dos negócios.

**Recomendações para os Conselheiros Consultivos e Administrativos**

Procurem exaltar a visão estratégica e a importância das Tecnologias da Informação, bem como um serviço jurídico especializado, como componente indissociável dos negócios. É fundamental que qualquer plano de negócio tenha como alicerce o uso de tecnologias para se concretizar, além do respaldo jurídico para garantir

a prevenção de passivo judicial. O envolvimento imediato da área de TIC das organizações nas decisões estratégicas e operacionais com respaldo jurídico é indiscutível.

Busquem conscientizar os executivos de que a Gestão do Capital Humano tendo como meta o preparo dos colaboradores para o enfrentamento de falhas de processos, crises operacionais e de continuidade, inclusive a conscientização das responsabilidades legais envolvidas e da crescente proliferação do Crime Cibernético, é fundamental e é dever de todos, não só do RH.

Orientem os tomadores de decisão da organização quanto aos riscos de fraudes, sejam Ocupacionais ou Cibernéticas, e da necessidade de efetivas ações preventivas.
Direcionem os diretores a investir na melhoria gradativa da transformação organizacional, incrementando, na cultura dos colaboradores, a compreensão e a responsabilidade quanto ao uso de recursos tecnológicos e da Internet.

Recomendem o desenvolvimento de instrumentos mandatórios, como Códigos de Conduta, Normas Internas, Procedimentos Operacionais, elaborados por profissionais especializados, incluindo respaldo jurídico, que sejam documentados e operacionalizados para garantir o entendimento e a aceitação dos colaboradores.
Promovam a compreensão da necessidade de monitorar processos e governar as pessoas que são responsáveis pelo cumprimento de normas e procedimentos da organização. Somente com uma monitoração perceptível e integrada a controles e processos transparentes de governança, será possível melhorar o desempenho, garantir um nível de segurança razoável e buscar os caminhos da sustentabilidade.

### 10.2 Diretoria Executiva

De modo geral, os Diretores Executivos das organizações são, efetivamente, os responsáveis pelo dia a dia operacional na condução dos negócios, além de serem incumbidos da implantação das políticas e metas estabelecidas pelo Conselho Consultivo ou de Administração, caso estejam estabelecidos. Portanto, a diretoria executiva possui a missão de operacionalizar os negócios de maneira híbrida entre as abordagens estratégicas e táticas.

O papel da diretoria executiva é vital para as organizações, pois é propulsora dos negócios, e possui a missão de fazer a organização operar. Compete à diretoria aplicar e fazer cumprir diversos requisitos fundamentais. Entre eles, estão todos os aspectos operacionais que possam proteger a organização e dar-lhe um nível aceitável de Segurança tecnológica, física e jurídica, ou seja, em todos os sentidos; logo, a Segurança é uma missão fundamental.

### Recomendações para os Diretores Executivos

Deve haver consenso entre os integrantes do corpo diretivo de que a proteção da organização, em todos os aspectos, permita um nível de segurança adequado. Segurança não é só missão da área de Segurança ou de TIC, mas responsabilidade de todos.

A diretoria executiva deve promover com seriedade a produção de políticas rígidas e consistentes para o alcance da prevenção contra fraudes e segurança da informação em todos os processos, sejam eles manuais informatizados ou difundidos através de redes locais, remotas ou na WEB.

O corpo de diretores executivos deve se policiar e ser coerente com suas próprias determinações e práticas estabelecidas, através de políticas, normas e procedimentos, dando exemplo aos colaboradores no cumprimento das mesmas. Não pode haver regras

de prevenção e segurança que só sirvam aos empregados.

### **10.3** Demais Níveis de Gestores

Genericamente, definimos Gestores como todos os profissionais que lideram subordinados hierárquicos ou não, mas tomam decisões e, portanto, fazem gestão, possuindo um papel fundamental na aplicação das estratégias executivas e determinações gerenciais.

Existem diversas denominações para gestores, tais como: chefe, coordenador, supervisor e outros, porém o mais importante não é o título, mas a capacidade de liderança desse profissional, pois lhe compete fazer com que sejam cumpridas as determinações superiores e acompanhar os processos operacionais e seus controles.

No que tange ao tema Segurança Corporativa, os Gestores são responsáveis por materializar as ações de prevenção e proteção, pela obtenção dos níveis de segurança esperados e pelas práticas dos demais colaboradores das organizações.

Para esses gestores é necessário o conhecimento em:

- Dos riscos de segurança que possam afetar a organização.
- Do impacto das falhas de segurança para os resultados da organização.
- Certificações em políticas, normas e procedimentos internos sobre a segurança da organização.
- Conhecimento das suas responsabilidades sobre monitoramento e direcionamento dos colaboradores em atender os requisitos de segurança.
- Identificar incidentes de segurança em todos os processos, inclusive os de segurança da informação, fraudes ocupacionais e fraudes cibernéticas, bem como saibam como reportá-los rapidamente aos responsáveis por mitigá-los.

### 10.4 Colaboradores

Definimos como Colaborador todo e qualquer empregado de uma organização, não importando o nível hierárquico. Dessa feita, as recomendações valem para todos os profissionais das organizações.

Todo e qualquer integrante da organização que utilize recursos tecnológicos com o fim de realizar seu trabalho, deve sempre estar consciente de suas responsabilidades na manutenção da segurança corporativa, e na garantia da continuidade dos negócios para a preservação do emprego e do progresso social.

As **recomendações** para Colaboradores compreendem:

- Conhecer os perigos no uso da Internet.
- Ter consciência de estar exposto ao furto de identidade e de informações pessoais e empresariais, através de vírus, *Spyware*, *Spam*, *Phishing Scan* e outros ataques. Portanto, é sua missão atualizar as ferramentas de proteção antes de se conectar as Redes com dispositivos próprios. Caso perceba que algum dispositivo da empresa não esteja com tais ferramentas atualizadas, deve comunicar à área responsável quando a empresa determinar que somente ela estivesse autorizada a fazer a correção.
- Saber identificar *softwares* defeituosos ou não confiáveis, com falhas de segurança que possam expor a organização a riscos.
- Ser responsável por identificar o uso de sistemas operacionais e *softwares* antigos ou desatualizados, entendendo seus riscos. Se o equipamento for da empresa, a

responsabilidade em atualizar é dela, se for do próprio colaborador, é de sua própria missão mantê-lo atualizado.
- Concordar expressamente sobre a permissão de acesso a equipamentos de mobilidade pessoais (*smartphones*, *tablets*, *notebooks*) usados no trabalho. Em se tratando de equipamentos pertencentes à empresa, ela deverá esclarecer e dar ciência ao empregado sobre as regras para seu uso e monitoramento.
- Estar consciente da responsabilidade administrativa e legal de armazenar dados em seus equipamentos por estar expostos ao envolvimento com dados indesejáveis, tais como aqueles de pornografia, racismo, terrorismo, pedofilia etc., além das demais condutas tipificadas no Código Penal (BRASIL, 1940).

### 10.5 Prestadores de Serviços e Parceiros

Prestador de Serviços é o profissional, ou a equipe de profissionais, que realiza trabalhos a título de venda da mão-de-obra física ou intelectual para terceiros. Na prática, muitas das tarefas específicas das organizações modernas são realizadas por profissionais prestadores de serviço. A relação entre o prestador de serviço (pessoa jurídica) e a empresa onde prestam os serviços sempre é contratual. Normalmente, são chamados de "terceirizados".

Ao longo do tempo ou mediante relacionamentos comerciais mais abrangentes, os prestadores de serviços, muitas vezes, qualificam-se como parceiros, embora juridicamente sejam relações distintas. As parcerias também podem ser societárias, através das quais a relação de sociedade jurídica é estabelecida entre as partes. De qualquer forma, prestadores de serviços e parceiros são, na prática, pessoas que trabalham na organização ou fazem parte do time de trabalho para alcance dos objetivos empresariais.

Nesse contexto de segurança corporativa, esses profissionais, sejam denominados prestadores de serviços ou parceiros, sempre estarão sujeitos às mesmas regras aplicadas a todos os colaboradores da organização.

Como **recomendações** para prestadores de serviços e parceiros devem:

- Cumprir todas as normas legais e técnicas vigentes no país, sobre saúde, segurança do trabalho e meio ambiente, respondendo pelos atos praticados decorrentes da não observância das referidas normas.
- Acatar, por assinatura, o Termo de Responsabilidade Individual, elaborado especificamente para prestadores de serviços e parceiros, e atender a políticas, normas e procedimentos da organização para a qual trabalham. A responsabilidade dos terceirizados é similar à responsabilidade dos colaboradores CLT da organização, com responsabilidade objetiva por seus empregados diretos e indiretos.
- Seguir os preceitos do código de conduta da empresa para a qual prestam serviços finais. Por prevenção jurídica, recomenda-se que o tratamento em documentos seja feito de forma separada, uma vez que pode influenciar uma possível agregação a um dos requisitos do vínculo empregatício.

## 11. LEGISLAÇÃO

### 11.1 Marco Civil

No mês de abril de 2014, foi sancionada a Lei nº 12.965/2014 (BRASIL, 2014),

que estabelece princípios e garantias, direitos e deveres para o uso da Internet no Brasil, com a finalidade de regulamentar não apenas a oferta de serviços, mas também o seu uso de forma geral, garantindo direitos e obrigações não apenas dos cidadãos, mas também das empresas.

No que se refere ao âmbito corporativo, cabe esclarecer que as empresas que oferecem aplicativos pela Internet passaram a ser obrigadas a promover a guarda dos registros que permitem a identificação de usuários, ou seja, provedores de aplicações de Internet deverão garantir a guarda dos seus registros de acesso pelo prazo de seis meses.

Também com relação às empresas que fornecem conexão à Internet, o administrador do sistema autônomo é obrigado a armazenar os registros de conexão pelo prazo de um ano.

Em ambas as situações, os registros deverão ser armazenados sob sigilo, em ambiente controlado e de segurança, e poderão ser fornecidos mediante determinação judicial decorrente de solicitação de autoridade policial, administrativa ou do Ministério Público.

Na perspectiva do cenário corporativo, pode-se vislumbrar que a lei define como administrador de sistema autônomo a pessoa física ou jurídica que administra blocos de IP específicos e o respectivo sistema autônomo de roteamento, devidamente cadastrada no ente nacional responsável pelo registro e distribuição dos endereços IP, geograficamente referentes ao país.

É sabido que as grandes e médias corporações, normalmente, possuem blocos de IP alocados, cuja administração e cuja distribuição interna são feitas pela própria empresa, podendo, conforme entendimento de alguns advogados, ser caracterizados como um administrador de sistema autônomo.

Diante desse cenário, não apenas os provedores de acesso à internet, mas também as empresas que gerenciam blocos de IP alocados para sua organização, devem garantir a guarda das informações de identificação pelo prazo mínimo de um ano.

Na hipótese da inviabilidade em utilizar o critério do valor do faturamento bruto da pessoa jurídica, a multa aplicada será no valor entre R$ 6.000,00 (seis mil reais) e R$ 60.000.000,00 (sessenta milhões de reais).

Para aplicação das sanções previstas na lei, é necessário considerar inúmeros aspectos, entre eles: a gravidade da infração, a vantagem auferida, sua consumação ou não, e a situação econômica, bem como as hipóteses elencadas nos incisos VII e VIII do artigo 7o, os quais definem que a cooperação da empresa e a existência de mecanismos e procedimentos internos de integridade e incentivo à denúncia passam a ser de suma importância.

Nesse cenário, os dispositivos supramencionados estão definitivamente ligados à Segurança da Informação, uma vez que, atualmente, todas as ações e comunicações acabam por utilizar recursos tecnológicos, de modo que o registro e armazenamento de informações, o rastreamento de acessos e o manuseio de informações, entre outros, poderão ser cruciais para minimizar uma possível sanção a ser aplicada à empresa.

No âmbito federal, o decreto nº 8.420/2015 regulamenta a respectiva lei, sendo que apresenta, no capítulo IV, que o programa de integridade deve ser estruturado, aplicado e atualizado de acordo com as características e riscos atuais das atividades de cada pessoa jurídica, acrescentando no art. 42 os parâmetros e condições de avaliação para existência e aplicação do programa de integridade os quais podemos transcrever abaixo:

Ressaltamos que a empresa tem responsabilidade objetiva por seus empregados no exercício de sua função, devendo a empresa promover uma análise de risco para que

possa determinar, em seu cenário, qual o melhor período de tempo para fazer a guarda dessas e de outras informações, assim como qual a necessidade de armazenamento por prazo maior do que o previsto no Marco Civil. Nesse sentido, sugere-se a criação de uma tabela de temporalidade.

Ademais, a respectiva Lei tem seu foco e impacto mais acentuado para empresas que prestam serviços digitais, ou seja, oferecem serviços *on-line*, de forma que, por exemplo, uma empresa estrangeira que ofereça seus serviços *on-line*, os quais possam ser acessados em território brasileiro, está obrigada a atender ao Marco Civil.

Dessa forma, no que se refere a serviços digitais, seu impacto é notório em relação ao consumidor tratando-se da isonomia em relação a acessos e conteúdos, coleta, guarda, compartilhamento e segurança das informações solicitadas aos usuários, entre outras questões, sendo necessária a atualização de Termos de Uso, Políticas de Privacidade e Contratos.

Por fim, destaca-se que há um impacto direto em relação à guarda de informações diante de um cenário em que, até então, tal prática ocorria por prevenção, a fim de atender entendimentos jurisprudenciais. Assim, de forma mais amena, passa a ser tratado em dispositivo legal.

### 11.2 Lei Anticorrupção

No dia 29 de janeiro de 2014, entrou em vigor a Lei nº 12.846/2013 – Lei Anticorrupção (BRASIL, 2013b), a qual versa sobre a responsabilização administrativa e civil de pessoas jurídicas pela prática de atos contra a administração pública, nacional ou estrangeira.

Até então, ocorrendo investigações, as empresas alegavam se tratar de ações isoladas de um ou mais colaboradores. Contudo, com a lei atual, esse cenário muda radicalmente, ou seja, independente de culpa ou dolo e, ainda que a empresa e seus gestores não tenham sequer ciência da ocorrência, serão ambos responsabilizados pelos atos de seus colaboradores, ressaltando que a responsabilidade da pessoa jurídica não exclui a responsabilidade individual da pessoa física.

No tocante à sanção da empresa na esfera administrativa, poderá ser aplicada multa, no valor de 0,1% (um décimo por cento) a 20% (vinte por cento) do faturamento bruto do exercício anterior ao da instauração do processo administrativo. Essa sanção não exclui a obrigação de reparar eventual dano decorrente.

Na hipótese da inviabilidade em utilizar o critério do valor do faturamento bruto da pessoa jurídica, a multa aplicada será no valor entre R$6.000,00 (seis mil) e R$60.000.000,00 (sessenta milhões de reais).

Para aplicação das sanções previstas na lei, é necessário considerar inúmeros aspectos, entre eles: a gravidade da infração, a vantagem auferida, sua consumação ou não, e a situação econômica, bem como as hipóteses elencadas nos incisos VII e VIII do artigo 7º, os quais definem que a cooperação da empresa e a existência de mecanismos e procedimentos internos de integridade e incentivo à denúncia passam a ser de suma importância.

Nesse cenário, os dispositivos supramencionados estão definitivamente ligados à Segurança da Informação, uma vez que, atualmente, todas as ações e comunicações acabam por utilizar recursos tecnológicos, de modo que o registro e armazenamento de informações, o rastreamento de acessos e o manuseio de informações, entre outros, poderão ser cruciais para minimizar uma possível sanção a ser aplicada à empresa.

No âmbito federal, o decreto nº 8.420/2015 regulamenta a respectiva lei, sendo que apresenta, no capítulo IV, que o programa de integridade deve ser estruturado,

aplicado e atualizado de acordo com as características e riscos atuais das atividades de cada pessoa jurídica, acrescentando no art. 42 os parâmetros e condições de avaliação para existência e aplicação do programa de integridade os quais podemos transcrever abaixo:

I - comprometimento da alta direção da pessoa jurídica, incluídos os conselhos, evidenciado pelo apoio visível e inequívoco ao programa;
II - padrões de conduta, código de ética, políticas e procedimentos de integridade, aplicáveis a todos os empregados e administradores, independentemente de cargo ou função exercidos;
III - padrões de conduta, código de ética e políticas de integridade estendidas, quando necessário, a terceiros, tais como, fornecedores, prestadores de serviço, agentes intermediários e associados;
IV - treinamentos periódicos sobre o programa de integridade;
V - análise periódica de riscos para realizar adaptações necessárias ao programa de integridade;
VI - registros contábeis que reflitam de forma completa e precisa as transações da pessoa jurídica;
VII - controles internos que assegurem a pronta elaboração e confiabilidade de relatórios e demonstrações financeiros da pessoa jurídica;
VIII - procedimentos específicos para prevenir fraudes e ilícitos no âmbito de processos licitatórios, na execução de contratos administrativos ou em qualquer interação com o setor público, ainda que intermediada por terceiros, tal como pagamento de tributos, sujeição a fiscalizações, ou obtenção de autorizações, licenças, permissões e certidões;
IX - independência, estrutura e autoridade da instância interna responsável pela aplicação do programa de integridade e fiscalização de seu cumprimento;
X - canais de denúncia de irregularidades, abertos e amplamente divulgados a funcionários e terceiros, e de mecanismos destinados à proteção de denunciantes de boa-fé;
XI - medidas disciplinares em caso de violação do programa de integridade; XII - procedimentos que assegurem a pronta interrupção de irregularidades ou infrações detectadas e a tempestiva remediação dos danos gerados;
XIII - diligências apropriadas para contratação e, conforme o caso, supervisão, de terceiros, tais como, fornecedores, prestadores de serviço, agentes intermediários e associados;
XIV - verificação, durante os processos de fusões, aquisições e reestruturações societárias, do cometimento de irregularidades ou ilícitos ou da existência de vulnerabilidades nas pessoas jurídicas envolvidas;
XV - monitoramento contínuo do programa de integridade visando seu aperfeiçoamento na prevenção, detecção e combate à ocorrência dos atos lesivos previstos no art. 5o da Lei no 12.846, de 2013; e
XVI - transparência da pessoa jurídica quanto a doações para candidatos e partidos políticos.
§ 1oNa avaliação dos parâmetros de que trata este artigo, serão considerados o porte e especificidades da pessoa jurídica, tais como:
I - a quantidade de funcionários, empregados e colaboradores;
II - a complexidade da hierarquia interna e a quantidade de departamentos, diretorias ou setores;
III - a utilização de agentes intermediários como consultores ou representantes comerciais;

IV - o setor do mercado em que atua;
V - os países em que atua, direta ou indiretamente;
VI - o grau de interação com o setor público e a importância de autorizações, licenças e permissões governamentais em suas operações;
VII - a quantidade e a localização das pessoas jurídicas que integram o grupo econômico; e
VIII - o fato de ser qualificada como microempresa ou empresa de pequeno porte.
§ 2o A efetividade do programa de integridade em relação ao ato lesivo objeto de apuração será considerada para fins da avaliação de que trata o caput.
§ 3o Na avaliação de microempresas e empresas de pequeno porte, serão reduzidas as formalidades dos parâmetros previstos neste artigo, não se exigindo, especificamente, os incisos III, V, IX, X, XIII, XIV e XV do caput.
§ 4o Caberá ao Ministro de Estado Chefe da Controladoria-Geral da União expedir orientações, normas e procedimentos complementares referentes à avaliação do programa de integridade de que trata este Capítulo.
§ 5o A redução dos parâmetros de avaliação para as microempresas e empresas de pequeno porte de que trata o § 3o poderá ser objeto de regulamentação por ato conjunto do Ministro de Estado Chefe da Secretaria da Micro e Pequena Empresa e do Ministro de Estado Chefe da Controladoria-Geral da União.

Tendo em vista que tanto a lei quanto o decreto não regulamentam diretamente a forma de obtenção das informações e controles tecnológicos que possam auxiliar nas investigações, a forma preventiva mais adequada de atuação das organizações será que as tais ações e controles tecnológicos se pautem nas boas práticas de mercado, atendendo às normas ISO 27001 (ABNT, 2013) e 27002 (ABNT, 2013).

O art. 16 da lei versa sobre o acordo de leniência, que representa um atrativo para as empresas que o celebrarem, tendo em vista que essas serão isentadas das sanções previstas no inciso II do art. 6o e inciso IV do art. 19 do respectivo dispositivo legal, ainda cabendo redução de até 2/3 da multa. No entanto, tal acordo não as exime do dever de reparar o dano decorrente da prática corruptiva. Frisa-se que os efeitos do acordo serão estendidos a todas as empresas pertencentes ao mesmo grupo.

A responsabilidade administrativa não exime a empresa da responsabilidade judicial, uma vez que os órgãos indicados na lei poderão ajuizar ação contra a respectiva empresa, requerendo as sanções previstas no art. 19, tais como:

I – perdimento dos bens, direitos ou valores que representem vantagem ou proveito, direta ou indiretamente, obtido da infração; II – suspensão ou interdição parcial de suas atividades; III – dissolução compulsória da pessoa jurídica; IV – proibição de receber incentivos, subsídios, subvenções, doações ou empréstimos de órgãos ou entidades públicas e de instituições financeiras públicas ou controladas pelo poder público, pelo prazo mínimo de 1 (um) e máximo de 5 (cinco) anos. (BRASIL, 2013b).

Diante do cenário exposto, no tocante à Lei n. 12.846/2013, não há dúvidas sobre a necessidade de ações preventivas relacionadas à Segurança da Informação a fim de evitar que a empresa sofra incidentes relacionados à corrupção e, caso esse tipo de problema ocorra, como modo de fazer com que a empresa possa ter mecanismos para obter as informações e provas necessárias para, de forma célere e eficaz, contribuir com a justiça, minimizando, inclusive, as sanções cabíveis.

### 11.3 Lei n. 12.737/2012

A Lei nº 12.737/2012 (BRASIL, 2012) dispõe sobre a tipificação criminal de delitos informáticos e estabelece os seguintes termos, com relação à invasão de dispositivo informático:

Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita.
Pena – detenção, de 3 (três) meses a 1 (um) ano, e multa. (BRASIL, 2012).

O respectivo artigo estabelece que uma invasão de dispositivo informático será considerada se ocorrer invasão mediante violação indevida de mecanismo de segurança. Alguns advogados entendem que a violação indevida caracteriza-se pelo simples acesso sem permissão; contudo, existe corrente contrária que defende não existir a necessidade de barreiras sólidas, como quebra de senhas, ou qualquer outro sistema de segurança digital.

A questão no ambiente corporativo é que a empresa deve se preparar para promover a coleta das evidências digitais para a materialização do conjunto probatório, de forma que, ao sofrer qualquer tipo de invasão, possa obter as provas necessárias para garantir, em juízo, a comprovação da conduta e, por consequência, romper as barreiras que possam atrapalhar a imputação do fato delituoso ao autor do crime.

É importante ressaltar que, de forma autoexplicativa, o mesmo artigo versa também:

§ 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput. (BRASIL, 2012).

Outro aspecto que merece ser colacionado diz respeito à Lei estabelecer punição em desfavor daquele que interromper o serviço telemático, ou de informação de utilidade pública, impedir ou dificultar-lhe o restabelecimento.

### 11.4 Decreto *E-commerce*

O Decreto nº 7.962/2013 (BRASIL, 2013a) trata da contratação no comércio eletrônico, versando acerca de três pontos centrais, explicitados nos incisos do seu artigo 1º:

a. Direito à informação: conforme estabelecido no Código de Defesa do Consumidor (BRASIL, 1990), em seu artigo 6º, inciso III, representando um dos direitos básicos do consumidor à informação adequada e clara sobre produtos e/ou serviços, nos termos do artigo 2º, do Decreto em comento;
b. Atendimento facilitado ao consumidor: tendo em vista as informações falhas e inconsistentes, bem como a ineficiência dos canais de comunicação. O Decreto (artigo 4º) estipula regras para inclusão de informações contratuais, atendimento em meio eletrônico (chats, por exemplo) e ferramentas para segurança da navegação e das informações;
c. Direito de arrependimento: elencado no artigo 5º do Decreto, também previsto no Código de Defesa do Consumidor (BRASIL, 1990, Art. 49). Contudo, no ambiente virtual, é revestido por outras características, de forma que o ônus para comunicação às

instituições financeiras vinculadas à operação recai sobre a empresa fornecedora/prestadora.

Portanto, conforme disposto no artigo 2º, as empresas devem ficar atentas, pois, obrigatoriamente, deverão constar no *site* as seguintes informações:

I – nome empresarial e número de inscrição do fornecedor, quando houver, no Cadastro Nacional de Pessoas Físicas ou no Cadastro Nacional de Pessoas Jurídicas do Ministério da Fazenda;
II – endereço físico e eletrônico, e demais informações necessárias para sua localização e contato;
III – características essenciais do produto ou do serviço, incluídos os riscos à saúde e à segurança dos consumidores;
IV – discriminação, no preço, de quaisquer despesas adicionais ou acessórias, tais como as de entrega ou seguros;
V – condições integrais da oferta, incluídas modalidades de pagamento, disponibilidade, forma e prazo da execução do serviço ou da entrega ou disponibilização do produto; e
VI – informações claras e ostensivas a respeito de quaisquer restrições à fruição da oferta. (BRASIL, 2013a).

## 11.5 Regulação Geral de Proteção de Dados da União Europeia

A GDPR - General Data Protection Regulation (Regulamento Geral sobre a Proteção de Dados), tal como ficou conhecida mundialmente, ganhou grande notoriedade em função da sua eficácia extraterritorial, o que equivale dizer que a ela estão submetidos não só os cidadãos europeus residentes e domiciliados na Europa, bem como aqueles que não residindo na Europa, não abriram mão de sua nacionalidade.

Seu escopo fundamenta-se na coleta, armazenamento e tratamento de dados pessoais por empresas europeias ou que operem em território europeu.

Ou ainda, aquelas empresas situadas em qualquer localidade do globo terrestre que necessitem fazer transferência de dados de cidadãos europeus para qualquer outro país do mundo.

Do ponto de vista do mercado tecnológico, esta legislação impactou fortemente os negócios de milhares de empresas, vez que a maioria delas subsidia suas operações com base na coleta, armazenamento e tratamento de dados pessoais de seus usuários.

Isto posto e com a entrada em vigor desta legislação em 25 de maio de 2018, após um período de *vacatio legis* de vinte e quatro meses, a GMG INTERNET SERVICE LTDA. alinhou toda a sua documentação e suas práticas de acordo com o disposto nesta lei, estando assim compliant com a nova orientação legal sobre a matéria de proteção de dados pessoais.

## 11.6 Lei nº 13.709/2018

A Lei Geral de Proteção de Dados Brasileira foi sancionada em 14 de agosto de 2018 com a previsão de um período de vinte e quatro meses de *vacatio legis*, entrando em vigor, portanto, em 15 de fevereiro de 2020.

Seu escopo trata da coleta, tratamento e armazenamento de dados em toda e qualquer circunstância, seja pelo poder público, seja pela iniciativa privada.

O titular do dado passa a ter, dentre outras garantias, o direito de conhecer a

finalidade para a qual seu dado está sendo coletado, bem como a possibilidade de pedir a exclusão de seu dado em qualquer tempo pelo motivo que julgar oportuno.

Todos os modelos de negócio que pautam-se na coleta de dados de seus usuários passarão por ajustes para o cumprimento desta lei, de forma a respeitar todos os direitos por ela garantidos e não ultrapassar os limites legais por ela estipulados.

A GMG INTERNET SERVICE LTDA, neste momento, trabalha para adequar seus produtos a esta legislação e continuar honrando seu compromisso de conformidade com todo a legislação em vigor no território brasileiro.

## 12. Considerações finais

Este manual constitui-se fundamentalmente numa compilação da obra já citada na introdução, qual seja, o guia de Referência sobre Segurança Corporativa da Comissão de Direito Digital e *Compliance* da OAB/SP.

Tem sido utilizado por nossa equipe como o conjunto de princípios e normais legais e morais a que nossa empresa deve se submeter, bem como os produtos por nós desenvolvidos.

Sabemos que ainda há muito o que aperfeiçoar, mas estamos certos de que este é o caminho para a construção de uma empresa ética, digna e honrada, cuja reputação seja reconhecida por nossos gestores, colaboradores, parceiros e até concorrentes.

A frequente utilização deste material para embasar as muitas decisões que tomamos todos os dias, com certeza gerarão por parte de cada uma das pessoas críticas e sugestões para seu aperfeiçoamento. Todas estas contribuições serão analisadas e, de acordo com a pertinência de cada uma, incorporadas às próximas versões deste conteúdo.

Ressaltamos aqui nosso compromisso com o desenvolvimento tecnológico e sustentável do planeta, bem como com o progresso econômico e social de nosso país.

## REFERÊNCIAS


ABNT. **NBR ISO 22301:2013**. Substituta da ABNT NBR ISO/IEC 15999-2:2008. Segurança da sociedade – Sistema de gestão de continuidade de negócios – Requisitos (*Societal security – Business continuity management systems – Requirements*). 2013a. Disponível em: <http://www.abntcatalogo.com.br/norma.aspx?ID=257946>. Acesso em: 15 nov. 2014.

ABNT. **NBR ISO/IEC 27001:2013**. Substituta da ISO/IEC 27001:2005. Sistemas de gestão da segurança da informação – Requisitos (*Information security management systems – Requirements).* 2013b. Disponível: <http://www.abntcatalogo.com.br/norma.aspx?ID=306580>. Acesso em: 13 nov. 2014.

ABNT. **NBR ISO/IEC 27002:2013**. Substituta da ISO/IEC 27002:2005. Código de prática para controles de segurança da informação (*Code of practice for information security management).* 2013c. Disponível em: <http://www.abntcatalogo.com.br/norma.aspx?ID=306582>. Acesso em: 13 nov. 2014.

ABNT **NBR ISO/IEC 38500:2008**. Governança Corporativa de Tecnologia da Informação (*Corporate governance of information techonology*). 2009. Disponível em: <http://www.abntcatalogo.com.br/norma.aspx?ID=40015>. Acesso em: 13 nov. 2014.

BRASIL. Constituição da República Federativa do Brasil, de 05 de outubro de 1988. 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/ConstituicaoCompilado.htm>. Acesso em: 13 nov. 2014.

BRASIL. Decreto Lei n. 2.848, de 07 de dezembro de 1940. Código Penal. 1940. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848.htm>. Acesso em: 13 nov. 2014.

BRASIL. Decreto n. 7.962, de 15 de março de 2013.2013a. Disponível em: <http://www2.camara.leg.br/legin/fed/decret/2013/decreto-7962-15-marco-2013-775557-publicacaooriginal-139266-pe.html>. Acesso em: 13 nov. 2014.

BRASIL. Lei n. 8.078, de 11 de setembro de 1990. Código de Defesa do Consumidor. Dispõe sobre a proteção do consumidor e dá outras providências. 1990. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l8078.htm>. Acesso em: 13 nov. 2014.

BRASIL. Lei n. 9.279, de 14 de maio de 1996. Lei de Propriedade Industrial. Regula direitos e obrigações relativos à propriedade industrial. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l9279.htm>. Acesso em: 13 nov. 2014.

Regulamenta a Lei n. 8.078, de 11 de setembro de 1990, para dispor sobre a contratação no comércio eletrônico.

BRASIL. Lei n. 9.504, de 30 de setembro de 1997. Estabelece normas para as eleições. 1997. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l9504.htm>. Acesso em: 13 nov. 2014.

BRASIL. Lei n. 9.610, de 19 de fevereiro de 1998. Lei de Direitos Autorais. Altera, 1998. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l9610.htm>. Acesso em: 13 nov. 2014.

BRASIL. Lei n. 10.406, de 10 de janeiro de 2002. Código Civil. 2002. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/2002/l10406.htm>. Acesso em: 13 nov. 2014.

BRASIL. Lei n. 12.551, de 15 de novembro de 2011. Altera o artigo 6o da Consolidação

das Leis do Trabalho (CLT), aprovada pelo Decreto-Lei n. 5.452, de 1o de maio de 1943, para equiparar os efeitos jurídicos da subordinação exercida por meios telemáticos e informatizados à exercida por meios pessoais e diretos. 2011a. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12551.htm>. Acesso em: 13 nov. 2014.

BRASIL. Lei n. 12.737, de 30 de dezembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos. 2012. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em: 13 nov. 2014.

BRASIL. Lei n. 12.846, de 1o de agosto de 2013. Lei Anticorrupção. Dispõe sobre a responsabilização administrativa e civil de pessoas jurídicas pela prática de atos contra a administração pública, nacional ou estrangeira, e dá outras providências. 2013b. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12846.htm>. Acesso em: 15 nov. 2014.

BRASIL. Lei n. 12.850, de 02 de agosto de 2013. Define organização criminosa e dispõe sobre a investigação criminal, os meios de obtenção da prova, infrações penais correlatas e o procedimento criminal; altera o Decreto-Lei n. 2.848, de 07 de dezembro de 1940 (Código Penal); revoga a Lei n. 9.034, de 3 de maio de 1995; e dá outras providências. 2013c. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12850.htm>. Acesso em: 13 nov. 2014.

BRASIL. Lei n. 12.965, de 23 de abril de 2014. Marco Civil da Internet. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. 2014. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 15 nov. 2014.

BRASIL. Superior Tribunal de Justiça. Recurso Especial n. 844.736-DF. Recorrente: Gerson Alves de Oliveira Junior. Recorrido: WB Restaurante Ltda. 4a Turma. Relator: Desembargador convocado Honildo Amaral de Mello Castro. Julgamento: 27 de outubro de 2009. 2009. Acesso em: 10 nov. 2014.

BRASIL. Superior Tribunal de Justiça. Recurso Especial n. 1.186.616-MG. Recorrente: Google Brasil Internet Ltda. Recorrido: Alexandre Magno Silva Marangon. 3a Turma. Relatora: Ministra Nancy Andrighi. Julgamento: 23 de agosto de 2011. 2011b. Acesso em: 10 nov. 2014.

BRASIL. Supremo Tribunal Federal. Súmula 341, de 13 de dezembro de 1963. 1963. Disponível em: <http://www.stf.jus.br/portal/jurisprudencia/listarJurisprudencia.asp?s1=341.NUME. % 20NAO%20S.FLSV.&base=baseSumulas>. Acesso em: 13 nov. 2014.

COBIT Security Baseline: an information security survival kit. 2nd edition. [s.d.] Disponível em: <http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/COBIT-Security-Baseline-An-Information-Security-Survival-Kit-2nd-Edition1.aspx>. Acesso em: 15 nov. 2014.

COMISSÃO das Comunidades Europeias. **Livro verde**. Promover um quadro europeu para a responsabilidade social das empresas. Bruxelas, Bélgica, 2001. Disponível em: <http://molar.crb.ucp.pt/cursos/2%C2%BA%20Ciclo%20-%20Mestrados/Gest%C3%A3o/2011-13/EERS_1113/Terceira%20e%20Quarta%20Sess%C3%B5es/Livro%20verde-promover%20um%20quadro%20europeu%20de%20RSE.pdf>. Acesso em: 13 nov.2014.

GUIA de referência sobre ataques via Internet. Febraban, jun. 2000. Disponível em: <http://www2.dem.inpe.br/ijar/GuiaFebraban.pdf> Acesso em: 24 nov. 2014.

GUIA PAS 200:2011. **Crisis management** – Guidance and good practice. 2011.

Disponível em: <http://shop.bsigroup.com/ProductDetail/?pid=000000000030252035>. Acesso em: 24 nov. 2014.
ISO**. ISO 22313:2012**. Societal security. Business continuity management systems. 2012a. Disponível em: <http://www.abntcatalogo.com.br/norma.aspx?ID=194144>. Acesso em: 15 nov. 2014.
ISO. **ISO 22301:2012**. Societal security. Business continuity management systems – Requirements. 2012b. Versão em inglês, originária da ABNT NBR ISO 22301:2013. Disponível em: <http://www.abntcatalogo.com.br/norma.aspx?ID=90849>. Acesso em: 15 nov. 2014.
JORGE, Higor Vinicius Nogueira; WENDT, Emerson. **Crimes cibernéticos**: ameaças e procedimentos de investigação. Rio de Janeiro: Brasport, 2012.
NFPA 1600. Standard on disaster/emergency management and business continuity programs. 2013. Disponível em: <http://www.nfpa.org/codes-and-standards/document-information-pages?mode=code&code=1600&tab=about>.
Acesso em: 15 nov. 2014.
atualiza e consolida a legislação sobre direitos autorais e dá outras providências.
OLIVEIRA, Helena. Crime económico: a tempestade perfeita. **Portal VER**. 12 jan. 2012. Disponível em:
<http://www.jornaldenegocios.pt/especiais/contribuicoes_externas/gestao_responsavel/detalhe/crime_econoacutemico_a_tempestade_perfeita.html> Acesso em: 15 nov. 2014.
SWANSON, Marianne et al. Contingency planning guide for federal information systems. National Institute of Standards and Technology. **NIST Special Publication**, 800-34, May 2010. Disponível em: <http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf>. Acesso em: 15 nov. 2014.