# Fonte

Tecnologia da Informação na Gestão Pública

Ano 14 | Nº 18
Dezembro 2017

ISSN 1808-0715
Distribuição gratuita

prodemge

www.prodemge.gov.br

# Cibersegurança: educação digital e proteção de dados

# Melhorar

os padrões de eficiência dos serviços públicos estaduais sempre foi a razão de existir da Prodemge.

## Mas, nesses 50 anos, fizemos mais que isso.

Aproximamos o cidadão do Governo de Minas Gerais por meio da tecnologia e da inovação.

**Para isso, contamos com milhares de personagens que nos ajudaram a traçar esse caminho.**

**A Prodemge agradece a todos que estiveram presentes nestes 50 anos e reconhece que uma história de sucesso é feita de pessoas, parceria e muito trabalho.**

/prodemge
@prodemge

Rodovia Papa João Paulo II, 4.001, CEP 31630-901
Bairro Serra Verde - Belo Horizonte / MG
Prédio Gerais, 4°andar - Tel. (31)3915-4137
negocios@prodemge.gov.br - www.prodemge.gov.br

50 ANOS | prodemge |

MINAS GERAIS
DIÁLOGO EQUILÍBRIO TRABALHO

# Editorial

Na era da informação e do conhecimento em rede, vivenciamos os desafios da mediação tecnológica nas relações e processos que perpassam praticamente todas as instâncias de um cotidiano hiperconectado. De um lado, o exponencial desenvolvimento das tecnologias da informação e comunicação não cessa de nos maravilhar. Uma realidade que propicia ganhos em produtividade, tempo e comodidade, ao reconfigurar as formas como indivíduos, grupos sociais, corporações, instituições públicas, privadas e do terceiro setor interagem, prestam serviços e estabelecem os mais diversos tipos de relacionamento.

Por outro lado, essa realidade conformada por uma infinidade de dispositivos sociotécnicos e novos comportamentos defronta com impactos de natureza disruptiva. Dentre eles, as temáticas ligadas à segurança da informação impõem-se como uma pauta incontornável.

No plano do resguardo do direito à privacidade e da intimidade do cidadão, basta lembrar as horas que, conscientemente ou não, passamos em frente a uma tela ou câmera. A cada clique, comentário ou pesquisa realizada na web, deixamos rastros digitais que dizem muito sobre nós e também colocam a nossa própria segurança em xeque. Mas há um pano de fundo ainda mais elementar, o da garantia da integridade das infraestruturas que suportam o funcionamento desse aparato em rede, vital em nosso dia a dia.

É nesse sentido que a Prodemge, cumprindo seu dever institucional, faz da segurança da informação um dos pilares de sua atuação. Uma orientação refletida na 18ª edição da revista Fonte, integralmente dedicada à cibersegurança. Afinal, ataques cibernéticos de grandes proporções, causados por potentes malwares e ransomwares espalhados por hackers e bots, têm trazido danos às organizações não só no Brasil, mas em todo o mundo.

Empresas públicas e privadas têm apostado em processos e projetos que, de modo constante, contribuam para a proteção de seus dados. A Prodemge não foge a essa responsabilidade: como referência em Tecnologia de Informação e Comunicação em Minas Gerais, investe fortemente em cibersegurança. Exemplos disso são os vários procedimentos de proteção dos dados do seu Data Center, o qual armazena e processa as informações geradas pelo Estado; e a criação do Centro de Operações de Segurança (CTIS), com o intuito de monitorar, identificar e tratar os incidentes de segurança que ocorrem contra a rede corporativa do governo de Minas Gerais e de outros clientes.

Porém, apenas investimentos em ferramentas e tecnologias não são suficientes. É preciso também educar e alertar os colaboradores e as pessoas em geral sobre a importância de sua postura nessa batalha digital que veio para ficar. Nesta edição, você conferirá dicas de como pode proteger as informações nos ambientes profissional e pessoal. Esteja preparado!

Boa leitura!

**Diretoria da Prodemge**


**Expediente**
Ano 14 – nº 18 – Dezembro de 2017

Governador do Estado de Minas Gerais
Fernando Damata Pimentel
Secretário de Estado de Planejamento e Gestão
Helvécio Miranda Magalhães Júnior
Diretor-presidente
Paulo de Moura Ramos
Diretor de Sistemas
Gustavo Guimarães Garreto
Diretor de Gestão Empresarial
Gilberto Rosário de Lacerda
Diretor de Negócios
Gustavo Daniel Prado
Diretor de Infraestrutura e Produção
Pedro Ernesto Diniz

Conselho Editorial
Gustavo Daniel Prado
Lilian Noronha Nassif
Márcio Luiz Bunte de Carvalho
Marcos Brafman
Vanessa Fagundes

**EDIÇÃO EXECUTIVA**

Superintendência de Marketing
Gustavo Grossi de Lacerda
Gerência de Comunicação
Lívia Mafra
Produção editorial e gráfica
Press Comunicação Empresarial
(www.presscomunicacao.com.br)
Jornalista responsável
Letícia Espíndola
Edição
Luciana Neves
Redação
Ana Carolina Rocha, Geórgea Choucair, Luciana D'Anunciação e Luciana Neves
Projeto gráfico
Claudia Daniel
Diagramação
Anderson Oliveira e Claudia Daniel
Colaboração
Guydo Rossi e Júlia Magalhães
Revisão
Luciana Lobato
Impressão
Globalprint Editora Gráfica
Tiragem
5.000 exemplares
Periodicidade
Semestral

A revista Fonte visa à abertura de espaço para a divulgação técnica, a reflexão e a promoção do debate plural no âmbito da tecnologia da informação e da comunicação. O conteúdo dos artigos publicados nesta edição é de responsabilidade exclusiva de seus autores.

prodemge

Rodovia Papa João Paulo II, 4.001
Serra Verde - CEP 31630-901
Belo Horizonte - Minas Gerais - Brasil
www.prodemge.gov.br
atendimento@prodemge.gov.br

# Sumário

# Renato Marinho

## Backup de dados para enfraquecer os temíveis ataques de ransomware

Com larga experiência em cibersegurança, o pesquisador, professor e palestrante teve reconhecimento internacional ao revelar, em 2016, o Mamba

Arquivo pessoal

*Renato Marinho é chefe de pesquisas do Morphus Labs e incident handler (manipulador de incidentes) do SANS Internet Storm Center – um programa do SANS Technology Institute, formado por organizações de ensino e pesquisa, criado para monitorar a segurança da rede mundial de computadores.*

*A jornada dele na área de cibersegurança teve início em 2001, quando criou o Nettion, um dos primeiros firewalls a usar o conceito atual de UTM (Unified Threat Management – Gerenciamento Unificado de Ameaças). Com larga experiência na área, teve reconhecimento internacional pela pesquisa que revelou o Mamba, o primeiro ransomware de criptografia completa de discos em 2016. Atualmente, à frente da Morphus Labs, é responsável pelas áreas de pesquisa, inovação e desenvolvimento de novos produtos.*

*Mestre e doutorando em Informática Aplicada, defende a cópia de segurança, ou backup, dos dados como forma de pessoas e empresas recuperarem informações, caso sejam vítimas de ataques de ransomware, mas também como uma boa prática para enfraquecer o modelo de negócio dos ransomwares. Renato é também professor do curso de pós-graduação em Segurança da Informação da Universidade de Fortaleza, onde leciona a disciplina de Perícia Forense Computacional. Palestrante, já apresentou trabalhos em eventos nacionais e internacionais, como SANS Data Breach Chicago 2017, Ignite Cybersecurity Conference Vancouver 2017, BSides Delaware 2016, BSides Vienna 2016, WSKS Portugal 2013, Fórum Nacional de CSIRTs 2015/2017 e GTER/GTS 2014.*

**Fonte: O senhor é o descobridor do Mamba, ransomware que, em setembro de**

**2016, comprometeu servidores do mundo inteiro, causando incalculáveis prejuízos à economia de países como Estados Unidos e Índia, pois sequestra dados das vítimas e exige valor de resgate para que o usuário readquira acesso à própria máquina. Qual a importância dessa descoberta?**

**Renato Marinho:** Nos últimos três a quatro anos, os ciberataques utilizando malwares do tipo ransomware têm crescido de forma expressiva, a ponto de tornarem-se uma das principais ameaças atuais. Muito dessa rápida expansão se dá pelo atalho que esse modelo criou para a monetização de cibercrimes. Ao invés de roubar informações bancárias ou dados de cartões de crédito, por exemplo, que exigem um passo a mais para transformar o fruto do roubo em dinheiro, a extorsão mediante a ameaça da perda definitiva dos dados tem sido suficiente para que muitas das vítimas venham a pagar os resgates aos criminosos.

Ao longo desse tempo, as tecnologias de segurança, principalmente os antivírus, têm evoluído na identificação dessas ameaças, por meio da análise do seu comportamento. Ao identificarem uma aplicação, fazendo a codificação (criptografia) de arquivos em massa no computador, por exemplo, poderiam interrompê-la por apresentar um comportamento suspeito e semelhante ao de um ransomware, minimizando, assim, os prejuízos às vítimas e, consequentemente, as chances do recebimento do resgate por parte dos criminosos.

Paralelamente, visando burlar as técnicas de detecção, os ransomwares também evoluíram, e o Mamba foi uma demonstração disso. Ele foi o primeiro a, efetivamente, utilizar uma estratégia que chamamos de criptografia completa de discos ou full disk encryption (FDE). Isso quer dizer que, ao invés de criptografar os arquivos individualmente, um a um, a ameaça criptografa todo o disco de uma vez. Além de burlar algumas formas de proteção, essa maneira de agir causa alguns efeitos colaterais sérios para as vítimas, que sequer, podem interagir com o sistema operacional de seus computadores, uma vez que ficam completamente inoperantes. Em se tratando de ambientes corporativos, a interrupção dos computadores significa a paralisação de sistemas e aplicativos básicos e, consequentemente, da operação do negócio por tempo indeterminado.

**F: De forma detalhada, como se desenvolveu a pesquisa do Mamba?**

**R.M.:** A descoberta foi feita durante a resposta a um incidente com ransomware envolvendo uma grande multinacional contra o qual o Morphus Labs foi acionado para atuar, em setembro de 2016. A princípio, esse seria mais um incidente envolvendo esse tipo de ameaça, mas, quando vi a tela de pedido de resgate, notei que estávamos diante de algo diferente.

> *"Em se tratando de ambientes corporativos, a interrupção dos computadores significa a paralisação de sistemas e aplicativos básicos e, consequentemente, da operação do negócio por tempo indeterminado"*

Até então, era comum que os computadores infectados por ransomware criptografassem documentos importantes, como fotos, planilhas, textos, etc. e, ao final do processo, abrissem uma janela do Windows com uma mensagem de texto com as orientações para o pagamento de um resgate caso a vítima quisesse seus dados de volta. No caso do Mamba, a mensagem de resgate não aparecia em uma janela do Windows, mas antes mesmo da inicialização do sistema operacional, após o boot do computador.

Essa foi só a primeira surpresa do dia. Ao pesquisar na internet, por meio da conexão compartilhada do meu smartphone, uma vez que a da organização foi interrompida pelo ataque, não encontrei nada a respeito daquela ameaça no Google – talvez uma das poucas vezes que o Google não me trouxe resultados. Estávamos, portanto, diante de uma ameaça desconhecida, sem uma amostra do malware para análise, uma vez que o próprio estava criptografado junto aos dados da vítima e sem referências externas que pudessem nos dar indícios ou orientar na solução do incidente.

Quando lidamos com incidentes, uma das principais atividades do tratamento é identificar a extensão do problema, ou seja, descobrir o escopo do ataque. Somente aqueles computadores facilmente identificáveis foram alvos dos atacantes? Havia alguma porta de entrada que permitisse o retorno desses ao restabelecermos a conexão internet? Para darmos essas respostas, tivemos que avançar na investigação praticamente de olhos vendados.

Ao avançarmos na análise do ambiente de rede e seguir alguns rastros potenciais, após 18 horas de trabalho

ininterrupto, acabamos encontrando uma amostra do ransomware em um computador que não sofreu o ciclo de infecção completo. A ameaça foi depositada, mas não executada, e isso abriu espaço para a identificação do escopo do ataque, outras estações infectadas e mitigação de novos ataques, bem como para a pesquisa que se seguiu.

De volta ao Morphus Labs, durante o final de semana após o incidente, investi bastante tempo na análise do malware. Fiquei instigado pelo fato de estar lidando com algo até então desconhecido e pela possibilidade de colaboração com outras organizações que poderiam vir a passar pelo mesmo problema. Ao final desse trabalho, já na segunda-feira, dia 12 de setembro, eu havia escrito um artigo com todos os detalhes do ransomware que batizamos de Mamba, em uma analogia ao efeito paralisante do veneno da serpente africana homônima.

No próprio dia 12, publicamos o artigo e começamos uma interação com empresas e entidades internacionais no sentido de propagar a pesquisa que acabáramos de lançar. O objetivo era difundir a nova estratégia usada pelo ransomware de forma que as tecnologias de segurança viessem a lançar vacinas e minimizar as chances de novas vítimas. O conteúdo se espalhou rapidamente e, em poucos dias, os principais portais de cibersegurança internacionais passaram a noticiar a nova descoberta.

### F: Outro ransomware que abalou o mundo, neste ano, foi o WannaCry. No que esses ransomwares se diferenciam?

**R.M.:** O WannaCry deu um novo passo na evolução dos ransomwares. Dessa vez, não na forma de aplicação da criptografia dos dados, mas na propagação do malware entre os computadores de ambientes corporativos. Ao invés de ficar restrito ao computador incialmente infectado, o WannaCry era capaz de varrer o ambiente de rede procurando por novas vítimas e se multiplicar por meio da exploração de uma grave falha do Microsoft Windows, que, apesar de contar com uma correção à época, muitas empresas ainda não a haviam aplicado.

A combinação da capacidade de multiplicação com a grande quantidade de computadores desatualizados resultou em uma mistura explosiva. Empresas ao redor do mundo tiveram prejuízos milionários com a interrupção de seus negócios – muito disso devido ao tempo exigido pelos procedimentos de aplicação da atualização do Windows.

### F: O ransomware é, atualmente, uma das principais ameaças globais na área de segurança da informação. Como as empresas e as pessoas comuns podem se proteger?

**R.M.:** Os ransomwares continuam entre as principais preocupações das organizações no tema cibersegurança. Com a migração dos ataques individuais para os ataques em massa, como os realizados pelo WannaCry e NotPetya este ano, a questão não é mais recuperar o backup de uma ou duas estações. Passamos a falar de hospitais inteiros paralisados devido a ataques de ransomware, com prejuízos que, nesse caso, podem extrapolar os financeiros.

Uma das principais armas contra essa ameaça continua sendo a cópia de segurança, ou backup, dos dados. Assim, caso a pessoa ou empresa venha a ser vítima, a recuperação do backup será suficiente. Além de facilitar a recuperação, essa boa prática enfraquece o modelo de negócio dos ransomwares. Com a progressiva redução dos rendimentos, é provável que o modelo venha a perder força e tenhamos uma redução desse vetor de ataque. Nada impede, infelizmente, que os ransomwares evoluam para novas formas de extorsão e emprego de novas tecnologias, como o machine learning (aprendizado de máquina), tão utilizado recentemente nas tecnologias de defesa.

### F: Quais são os principais desafios para impedir ataques de proporções mundiais?

**R.M.:** Um deles é a quantidade de dispositivos vulneráveis ou susceptíveis a ataques. Vamos pegar o exemplo dos ataques de negação de serviço, ou os chamados DDoS (Distributed Denial of Service) attacks. Aqui, os cibercriminosos contaminam milhares de computadores e, mais recentemente, os dispositivos IoT (internet das coisas), formando as chamadas botnets, que podem ser comandadas para execução de ataques em massa. Um bom exemplo foi o que aconteceu em outubro de 2016, quando a Mirai Botnet gerou um volume de tráfego de aproximadamente 1.2 TB contra um provedor global de DNS (serviço de domínios de internet), resultando na interrupção de serviços de gigantes como Netflix e Twitter.

> ***"Passamos a falar de hospitais inteiros paralisados devido a ataques de ransomware, com prejuízos que, nesse caso, podem extrapolar os financeiros"***

Nesse cenário, a solução passa pela ação de cada pessoa ou empresa de manter seus dispositivos seguros e atualizados. Não adianta que uma pequena parcela o faça. Enquanto houver dispositivos vulneráveis, suficientes para provocar um grande impacto, não teremos resolvido esse problema. Esse, portanto, é um dos grandes desafios para se impedir ataques de proporções mundiais.

## F: Quais foram os ganhos profissionais que o senhor e a sua empresa obtiveram com essa descoberta?

**R.M.:** Acredito que as relações que foram estabelecidas ao longo das interações com outros pesquisadores e organizações nacionais e internacionais. O Morphus Labs, a área de pesquisas avançadas em cibersecurity da Morphus, passou a trocar experiências de forma consistente com essas entidades e passou a ser reconhecido como uma fonte de conteúdo respeitada sobre o tema. A exemplo dessa, outras de nossas pesquisas têm sido aceitas em importantes conferências, tais como a Botconf, que aconteceu em Montpellier, França, no começo de dezembro de 2017, na qual apresentei uma pesquisa que revelou uma grande Botnet P2P com computadores e dispositivos IoT sequestrados em 178 países prontos para atacar.

## F: Na condição de incident handler da SANS, o que o senhor poderia nos adiantar de novidades e tendências a respeito de cibersegurança?

**R.M.:** O grupo de Incident Handlers da SANS é um excelente exemplo dessa cooperação internacional da qual faço parte. Formado por 30 voluntários espalhados em várias partes do mundo, o grupo funciona como um termômetro para ameaças emergentes detectadas a partir de sensores espalhados na internet, da interação com a comunidade, que nos fornece amostras de ameaças ou potenciais ameaças e da experiência diária do próprio handler no seu dia a dia.

Além da evolução natural das ameaças que conhecemos, tais como malwares bancários e ransomwares, temos percebido um aumento dos alvos envolvendo moedas digitais. O alto valor que o bitcoin e outras moedas têm alcançado tem atraído a atenção dos cibercriminosos, que buscam roubar carteiras ou usar o poder de processamento dos computadores da vítima para fazer o que se chama de mineração de moedas. De forma resumida, a atividade de mineração é a forma utilizada para validar as transações e recompensar com moedas digitais aqueles que conseguem contribuir, em rede, em uma espécie de loteria. Dessa forma, para aumentar a chance de receber a recompensa, muitos malwares estão usando milhares de computadores infectados para esse fim.

## F: O senhor desenvolveu outro trabalho sobre acesso a redes wireless pública. O que mais te surpreendeu no resultado?

**R.M.:** Apesar da grande oferta que temos atualmente de redes 3G/4G com velocidades mais elevadas, as redes WiFi ainda são bastante atrativas para os usuários de internet. Por isso, é muito comum que estabelecimentos comerciais, shopping centers e restaurantes ofereçam essa cortesia aos seus clientes.

Acontece que essa conveniência pode oferecer alguns riscos aos usuários. Por exemplo, caso a rede não seja bem configurada ou bem gerenciada, há alta probabilidade de que terceiros venham a coletar dados sensíveis dos usuários da rede sem que eles percebam e sem que tenham que instalar um malware nos dispositivos. Na pesquisa que realizamos de forma experimental em 2015, o objetivo era verificar exatamente a susceptibilidade dos usuários a esses riscos.

De propósito, configuramos o falso hotspot utilizado na pesquisa de forma que o usuário que o acessasse recebesse avisos de segurança, simulando um ataque pouco sofisticado, e, ainda assim, obtivemos uma alta taxa de usuários que aceitaram o risco. Em média, 75% das pessoas aceitaram, talvez por desconhecerem o risco, acessar uma rede insegura.

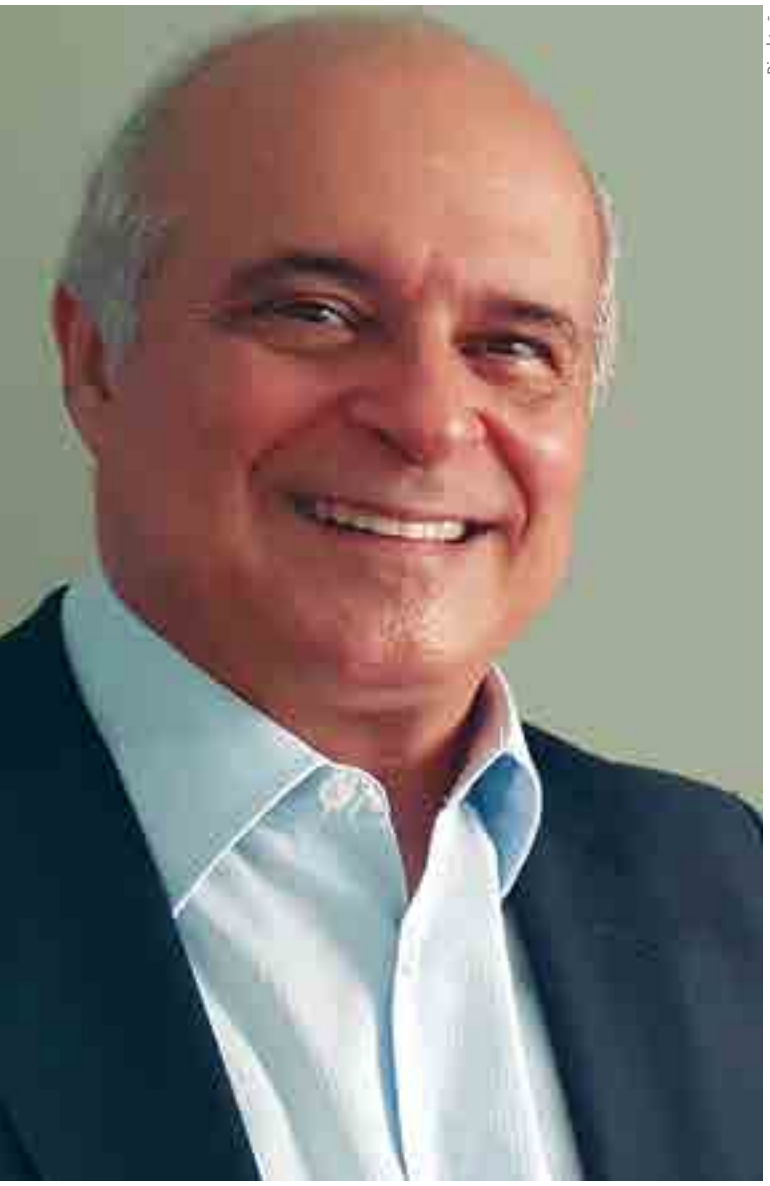
## F: De que forma o usuário pode proteger os próprios dados, já que muitos são afoitos em capturar uma rede mais rápida e de graça?

**R.M.:** Em redes públicas, a melhor estratégia é usar serviços de VPN (Virtual Private Network), que estabelecem uma conexão segura entre o dispositivo do usuário e o servidor do serviço de VPN. Dessa forma, minimiza-se bastante o risco de captura de dados por terceiros. Adicionalmente, os usuários devem ficar atentos aos alertas de segurança emitidos pelo navegador ou pelos aplicativos de internet e lê-los com atenção. Caso sejam requisitados para aceitar um certificado inválido ou mensagens relacionadas a isso, o ideal é interromper o acesso e continuar posteriormente a partir de uma conexão mais segura.

# Glicério Ruas

## Educação para redução de riscos cibernéticos

Integrante de diversos projetos para redução de ciberataques, o empresário afirma que as corporações já dedicam uma parcela de seus orçamentos de tecnologia para a segurança



Divulgação

*O empresário e administrador de empresas José Glicério Ruas Alves, 62 anos, participou de diversos projetos de contenção de ataques cibernéticos nos últimos meses. Ele é fundador e CEO de uma empresa criada em 1992, pioneira em software livre em Minas Gerais, especializada em segurança da informação e uma das maiores fornecedoras de segurança de tecnologia da informação e comunicação para órgãos do Estado de Minas Gerais.*

*Nesta entrevista, Glicério traça um panorama dos mais recentes ataques cibernérticos e avalia a postura do Brasil frente a esse tema e sua parceria com outros países para lidar com o desafio da cibersegurança. Para ele, é urgente a necessidade de cidadãos, empresas e governos reservarem recursos para a proteção adequada dos próprios dados, sob pena de amargarem prejuízos incalculáveis.*

**Fonte: Resgatando um pouco da história, quando surgiu o conceito de cibersegurança como conhecemos hoje e em que país?**

**Glicério Ruas:** Para contextualizar o que, hoje, tratamos como um termo "íntimo", acho importante explicar a origem da palavra cibernética. Quando iniciei o curso de Administração de Empresas na Universidade Federal de Minas Gerais (UFMG), em 1976, tomei conhecimento de uma ciência que estudava os mecanismos de comunicação e de controle nas máquinas e nos seres vivos, do modo como se organizam, regulam, reproduzem, evoluem e aprendem, baseados na noção estruturalista da sociedade, vista como um sistema de comunicação que se fundamenta na troca de mensagens culturais de tipo binário.

Hoje, chamamos de "ciber" tudo o que permeia a computação, seja em um só local, seja espalhado em diversos locais, como bairros, cidades, estados e países.

Atualmente, cibersegurança é um termo amplamente utilizado, sendo associado a outras palavras, como ciberespaço, ciberameaças, cibercriminosos, etc. Temos uma percepção natural sobre o que ele representa. Em algumas situações, o termo é utilizado como sinônimo de segurança da informação, segurança da informática ou segurança de computadores.

Ciber provém do diminutivo da palavra cybernetic (cyber), que, em português, significa alguma coisa ou algum local que possui uma grande concentração de tecnologia avançada, em especial computadores, internet, etc.

Quanto ao pioneirismo, existem reivindicações de diversos concorrentes de terem desenvolvido o primeiro produto antivírus. Talvez, a primeira publicamente conhecida neutralização de vírus de PC foi realizada pelo europeu Bernt Fix, autor do primeiro antivírus de computador documentado, no início de 1987. A correção neutralizava uma infecção do vírus Viena. O programa só estava disponível em polonês. Em 1988, surgiu o primeiro antivírus, desenvolvido por Denny Yanuar Ramdhani, em Bandung, Indonésia, a imunizar o sistema contra o vírus de boot Brain, paquistanês. Ele extraía o vírus do computador e, em seguida, imunizava o sistema contra outros ataques da mesma praga. Pouco tempo depois, a IBM lançou o primeiro antivírus comercial, sendo logo seguida por outras empresas, dentre as quais a Symantec e a McAfee, de olho no filão de ouro que esse mercado viria a representar. Elas acertaram em cheio, porque o número de malwares (vírus, worms, trojans, spywares e outros códigos nocivos) vem crescendo exponencialmente. Desde então, surgiram diversas empresas interessadas nesse mercado.

Com o advento da internet, a constante diminuição dos custos das telecomunicações e o barateamento dos dispositivos pessoais, os criminosos que utilizam esses elementos para causarem danos, os denominados cibercriminosos, vêm aumentando vertiginosamente em todo o mundo.

Hoje, vírus já não são os mais importantes causadores de estragos a pessoas, empresas e governos. Explorações de vulnerabilidades de aplicativos, sistemas operacionais, infraestrutura de segurança e redes estão entre os principais causadores de prejuízos. É nesse contexto que a cibersegurança tem se ampliado. Já não há mais barreiras geográficas entre os criminosos e os defensores.

> ***"Exploração de vulnerabilidades de aplicativos e sistemas operacionais, da infraestrutura de segurança e de redes está entre os principais causadores de prejuízos. É nesse contexto que a cibersegurança tem se ampliado"***

**F: Desde quando o Brasil trata de cibersegurança? Como começou e como se espalhou pelo governo e pelas empresas, independentemente do ramo e do tamanho?**

**G.R.:** Cibersegurança ainda não tem sido tratada com prioridade no Brasil. Alguns estudos indicam que mais da metade das empresas brasileiras não oferece educação em cibersegurança aos seus funcionários. Por outro lado, poucas empresas teriam admitido que fariam alguma ação sobre o assunto nos próximos tempos.

As organizações brasileiras precisam corrigir uma grande lacuna de comunicação entre as equipes de segurança e os executivos para se protegerem contra ataques avançados e roubo de dados, além de investir mais na educação dos funcionários.

A maioria dos profissionais brasileiros acredita que o roubo de propriedade intelectual, a violação envolvendo dados de clientes e a perda de receita por parada do sistema são os eventos mais preocupantes para a área de segurança. Mas boa parte das equipes de segurança de TI nunca comentou com os executivos das próprias empresas sobre questões de cibersegurança. Poucos profissionais brasileiros acreditam que as suas corporações investem o suficiente em pessoal e em tecnologia para evitar riscos cibernéticos.

Apesar disso, empresas privadas e governos têm instalado proteção para seus endpoints (equipamentos digitais que sejam pontos na rede, incluindo computadores e outros elementos de rede) e procurado serviços especializados

Alex Ferro

*Investimentos em cibersegurança foram realizados durante os Jogos Olímpicos e Paralímpicos Rio 2016*

externos como forma de transferência de conhecimento para suas equipes técnicas, que devem repassá-lo para os demais colaboradores.

Entretanto, sabemos que há outras formas de invasão e ataques, algumas silenciosas, que antivírus e proteção dos endpoints não enxergam, como ataques avançados e direcionados. Contra esses tipos de ameaças, as empresas brasileiras não têm se protegido adequadamente.

O maior patrimônio de uma empresa são suas informações, inclusive as armazenadas digitalmente. Mas tamanho não é documento no caso de cibersegurança, pois empresas pequenas também podem servir de trampolim para ataques a concorrentes e inimigos políticos, por intermédio de cibercriminosos. Por isso, pessoas e empresas brasileiras deveriam estar mais bem preparadas.

## F: Mesmo as grandes empresas não têm investido a quantidade que deveriam?

**G.R.:** No Brasil, algumas grandes empresas já dedicam uma parcela de seus orçamentos de tecnologia para segurança. O que não acontece nas pequenas e médias. Como no mundo real, os cibercriminosos querem as portas mais fáceis e essas empresas acabam caindo nessa situação com mais facilidade.

## F: O senhor poderia citar algum exemplo de medida real preventiva contra ataques no Brasil?

**G.R.:** Sabemos que a ciberguerra pode estar acontecendo nos bastidores. Dificilmente, nós, do povo, ficamos sabendo de detalhes. Porém, as nem tão recentes denúncias de Edward Snowden (ex-técnico da CIA, acusado de espionagem por vazar informações sigilosas de segurança dos Estados Unidos e revelar em detalhes alguns dos programas de vigilância que o país usa para espionar a população americana) fizeram o Exército brasileiro exigir, em seu edital para contratação de proteção de endpoints, que o fabricante se comprometesse, declarasse e demonstrasse que seu produto não possui backdoor, o que permitiria espionagem. O fabricante que não declarou foi desclassificado da licitação. Isso é uma demonstração de valorização da nossa soberania. Se nos importamos com isso, não permitimos a sua violação e podemos controlar e definir com quem não queremos nos vincular, já é um sinal de que podemos fazer nossa cibersegurança real.

## F: O Brasil conta com a parceria de quais países e de que forma isso acontece visando entender a atuação de criminosos virtuais?

**G.R.:** O Brasil ainda carece, na minha visão, de uma base de dados centralizada e oficial sobre ataques digitais. As informações que possuímos indicam que o número de ciberataques aumenta ano a ano, a maioria composta por tentativas de fraudes.

Em 2015, a Polícia Federal deflagrou, em Goiânia (GO) e Belo Horizonte (MG), a operação internacional Darkode, em parceria com o FBI. Policiais federais especialistas em investigações cibernéticas trabalharam diretamente com os maiores especialistas da Cyber Division do FBI e da Europol. Os agentes cumpriram mandados de prisão contra mais de 62 hackers identificados no mundo inteiro, na maior operação de cooperação internacional da área cibernética. Participaram desse trabalho unidades especializadas em crimes cibernéticos de 18 países, além do Brasil.

O fórum Darkode foi utilizado para a negociação criminosa de dados de cartões de crédito, ferramentas, credenciais, vulnerabilidades, lista de e-mails e todo tipo de informação que pudesse ser usada para a prática de crimes cibernéticos. A investigação identificou hackers brasileiros entre os maiores especialistas mundiais em crimes cibernéticos já presos pela PF. Os investigados brasileiros possuíam grande reputação entre os membros do Darkode, chegando a alcançar os níveis mais especializados do fórum.

Nos Jogos Olímpicos e Paralímpicos de 2016, o trabalho do Centro de Cooperação Policial Internacional (CCPI) foi conduzido pela Polícia Federal e operado com cerca de 250 policiais de 55 países, além de Interpol, Ameripol e Europol, reunidos em dois centros de comando e controle no Rio de Janeiro e em Brasília, que funcionaram entre os dias 1º de agosto e 19 de setembro daquele ano.

Foi a maior operação de cooperação policial internacional da história do Brasil e da própria Interpol. Participaram Angola, Argélia, Argentina, Austrália, Áustria, Bélgica, Canadá, Chile, Colômbia, Coréia do Sul, Dinamarca, Eslováquia, Eslovênia, Espanha, Estados Unidos, França, Holanda, Hungria, Iêmen, Índia, Itália, Japão, Malásia, México, Nigéria, Noruega, Nova Zelândia, Oman, Portugal, Catar, Reino Unido, Rússia, Suíça, Turquemenistão e Ucrânia. Nesses casos, há interesses comuns, ou seja, a proteção de seus atletas e concidadãos.

Isoladamente, por decisão estratégica, alguns produtores de soluções de segurança contratam analistas brasileiros de malware. O vírus do boleto, por exemplo, foi descoberto por um brasileiro analista de malware da Kaspersky Lab, empresa russa produtora de softwares de segurança. Isso não representa parceria entre governos, mas a decisão de conhecer, mais rapidamente, os malwares desenvolvidos por cibercriminosos brasileiros.

## F: Quais são as principais fraudes brasileiras e os impactos em outros países?

**G.R.:** A emissão de boletos bancários é muito comum nas cobranças no Brasil e os cibercriminosos desenvolveram e espalharam fraudes com boletos. Pesquisadores da RSA (empresa norte-americana que se dedica à criptografia) publicaram um relatório que revelou que as fraudes dos boletos custaram, em 2012, mais de 3,75 milhões de dólares para o Brasil e continuam causando prejuízos.

Recentemente, um velho conhecido voltou a atacar empresas no Brasil. Pesquisadores da Kaspersky detectaram uma nova onda do poderoso ransomware Mamba, famoso por ter interditado o transporte público de São Francisco (EUA), em 2016. O Mamba é particularmente danoso por criptografar o disco rígido inteiro, em vez de alguns arquivos. Ele é semelhante aos malwares Petya e Mischa, assim como o ExPetr, responsável pelo maior surto global dos últimos tempos.

Ainda não se sabe quem está por trás da nova onda de ataques contra companhias brasileiras. Negócios na Arábia Saudita também estão sendo afetados. Os pesquisadores da Kaspersky Lab afirmam que essa onda de sabotagem cibernética disfarçada de extorsão, por meio do Mamba, vai continuar. Ao contrário dos ataques do ExPetr, em que é improvável que as vítimas recuperem suas máquinas, talvez não seja o caso com o Mamba. O analista sênior de malware da Kaspersky no Brasil, Fábio Assolini, afirmou que o Mamba tem sido usado em ataques direcionados contra empresas e infraestruturas críticas, inclusive no Brasil. E alertou que, diferentemente das outras famílias de ransomwares, ele impossibilita o uso da máquina comprometida, exibindo o pedido de resgate e cifrando o disco por completo. O uso de um utilitário legítimo na cifragem é outra prova de que os autores visam causar o maior dano possível. Mas o relatório da Kaspersky Lab informa que não há nenhuma maneira de decodificar dados criptografados utilizando-se o DiskCryptor (ferramenta que criptografa arquivos do HD e mídias removíveis para proteger arquivos confidenciais), porque ele usa algoritmos de criptografia fortes.

## F: Os cibercrimes tendem mesmo a aumentar, considerando a ampliação de acesso à internet?

**G.R.:** Além da ampliação do acesso à internet, há a deseducação dos usuários. Outra razão é a quase garantia de anonimato do fraudador somada à facilidade de ganhos financeiros com as fraudes. Entre os ataques mais comuns para estimular uma ação ilícita ou servir de entrada para invasões destacam-se os de simulação de ambiente, como o phishing e o spoofing. Datas importantes para o varejo, como Black Friday, Dia das Mães e grandes eventos, como as Olimpíadas, são facilitadoras de crescimento dos ataques.

## F: Por que a Rússia é o país que mais sofre com ataques cibernéticos?

**G.R.:** Algumas pesquisas realmente indicaram isso. Talvez porque na Rússia exista muita gente capacitada. Nós, brasileiros, podemos estar pensando que não foi tão perto assim e nos despreocupamos. Mas, no Brasil, tivemos notícias de que os ciberataques levaram várias empresas e órgãos públicos a tirarem sites do ar e desligarem seus computadores.

**F: Israel é considerado grande referência em cibersegurança. No que esse país do Oriente Médio se diferencia do resto do mundo?**

**G.R.:** Israel tem uma vocação tecnológica histórica. O país apoia muitas iniciativas que traduzem avanços para a sociedade. Isso faz parte do programa de governo de Israel. O que é muito bom. Há uma decisão governamental de fortalecer a educação e preparar mão de obra especializada. Muitas empresas israelenses são destaques em suas áreas de atuação por disporem de técnicos e profissionais qualificados.

**F: Pesquisa da Security & Defence Agenda (SDA), um centro de estudos de Bruxelas dedicado à segurança cibernética, revela que as estratégias dos países estão longe de materializarem-se em efetiva segurança quando se trata de espionagem ou ciberataques. Por que essa desvantagem com os cibercriminosos?**

**G.R.:** De fato, a SDA constatou que os mocinhos, até para se protegerem, precisam obedecer a leis, enquanto os bandidos não seguem leis e compartilham informações entre eles, fortalecendo-se mutuamente. Quando as corporações públicas e privadas se conscientizarem de que tecnologias de prevenção custam menos do que o eventual remédio que vier a ser necessário, os prejuízos diminuirão.

**F: O que ainda veremos relacionado à ciberataques? O que esse crime ainda nos reserva? Qual o panorama mundial?**

**G.R.:** Veja um resumo do que vem acontecendo no mundo, nos últimos meses, em vários campos:

**Consultoria**: ataque cibernético à Deloitte, uma das quatro maiores empresas mundiais de consultoria, afetou clientes. O jornal britânico *The Guardian* informou que a empresa foi alvo de um ataque com um elevado grau de sofisticação que revelou e-mails e informações confidenciais de importantes clientes do setor tecnológico.

**Tecnologia:** dois milhões de usuários em todo o mundo instalaram versão infectada do programa de limpeza CCleaner. O CCleaner tinha sido criminosamente modificado para incluir uma componente de backdoor (que permite a intrusão de arquivos estranhos ou maliciosos num computador quando está ligado à internet e a instalação de ransomwares).

**CRM Corporativo:** ataque pôs em risco dados pessoais de 143 milhões de norte-americanos clientes da Equifax (um dos três maiores *bureaux* de crédito americano, que reúne e mantém informações de mais de 400 milhões de pessoas e empresas no mundo).

**Automóveis:** carros autônomos não serão vendidos nos Estados Unidos sem plano de cibersegurança, para que não sejam utilizados como armas por cibercriminosos.

**Usinas hidroelétricas**: hackers infiltraram-se no setor energético na Europa e nos Estados Unidos, com o objetivo de controlar a rede elétrica nas regiões ocidentais, para sabotar e programar cortes de eletricidade.

**Saúde humana:** meio milhão de pacemakers (um dispositivo implantado que regula eletronicamente os batimentos cardíacos, monitora o ritmo cardíaco e, quando necessário, gera um impulso elétrico indolor que desencadeia um batimento cardíaco) nos Estados Unidos vão ser atualizados para evitar ciberataques. A Food and Drug Administration (responsável pela proteção e promoção da saúde pública nos Estados Unidos) identificou uma vulnerabilidade no sistema de uma das marcas de pacemakers com ligação à internet em utilização no país.

**Televisão:** piratas informáticos voltaram a atacar e anteciparam o regresso de Curb Your Enthusiasm (sitcom norte-americano), prejudicando sua estreia.

**Jornalismo:** site da WikiLeaks foi atacado no dia em que revelou documentos da CIA, o que impediu que usuários tivessem acesso a novas informações sobre as práticas de espionagem dos Estados Unidos. O grupo de piratas responsável pelo ataque é famoso por se infiltrar nas contas das redes sociais de grandes empresas (como HBO, Netflix, Sony e Marvel) e de figuras públicas como os diretores executivos do Facebook e do Google.

**Justiça:** ciberataque atingiu computadores do Ministério Público de São José do Rio Preto. Alguns equipamentos apresentaram mensagens de que era necessário pagamento para acessar os arquivos (o que indicou o ataque de ransomware).

Além desses, o ciberataque mundial de 12 de maio de 2017, que afetou dezenas de países e fez hospitais públicos na Inglaterra cancelarem atendimentos e redirecionarem ambulâncias, também atingiu 14 estados do Brasil e o Distrito Federal. No Brasil, teriam tirado seus sites do ar a Petrobras; o Instituto Nacional do Seguro Social (INSS); os tribunais de Justiça de São Paulo, Sergipe, Roraima, Amapá, Mato Grosso do Sul, Minas Gerais, Rio Grande do Norte, Piauí, Bahia e Santa Catarina; o Ministério Público de São Paulo; o Itamaraty; e o Instituto Brasileiro de Geografia e Estatística (IBGE).

*Cibersegurança tornou-se um assunto de peso em todo o mundo*

## F: O que mais assusta os profissionais que convivem com esse assunto diariamente?

**G.R.:** No Brasil, não temos muitos profissionais especialistas em segurança em profundidade. Mas, mesmo os que têm menos experiência têm consciência de que, sem ferramentas de qualidade, não poderão fazer nada. O que mais assusta é a incapacidade de convencer os altos escalões sobre a necessidade de investimento em segurança. Perceberem, de braços cruzados, as ações de criminosos virtuais deixa-os irritados e inconformados.

## F: No que consiste uma política de cibersegurança?

**G.R.:** O principal fator de sucesso de uma política de segurança da informação é a educação dos usuários – uma corrente é tão forte quanto seu elo mais fraco. Também é preciso considerar a escolha de ferramentas de qualidade para facilitar o cumprimento das regras de uso dos recursos digitais.

A segurança da informação é constituída por cinco pilares: confidencialidade, integridade, disponibilidade, autenticidade e legalidade. A confidencialidade é a garantia de que as informações sejam acessadas somente por pessoas expressamente autorizadas e devidamente protegidas do conhecimento de terceiros. A integridade assegura que as informações estejam íntegras em todo o seu ciclo de vida. Já a disponibilidade faz com que as informações e os recursos de Tecnologia da Informação e Comunicação estejam disponíveis sempre que necessário e mediante a devida autorização para seu acesso e uso. A autenticidade é a prova que a informação seja fidedigna, capaz de gerar evidências não contestáveis sobre a identificação de quem a criou, editou ou emitiu. Por último, a legalidade é a garantia de que todas as informações sejam criadas e gerenciadas de acordo com as disposições do ordenamento jurídico em vigor no Brasil.

## F: Com a onda de dispositivos conectados, por meio da internet das coisas (IoT), o senhor acha que os usuários têm dado o mesmo grau de importância à segurança assim como consideram as funcionalidades dos aparelhos adquiridos?

**G.R.:** Muitas vezes, não nos lembramos de que as "coisas" já estão conectadas e não estão sendo tomados cuidados de segurança no projeto, na sua implementação e adoção. Carros, lâmpadas, TVs, eletrodomésticos e equipamentos médicos são sistemas complexos e completos, possuem sistema operacional, aplicações web, permitem acesso remoto, etc. Outro exemplo antigo é o ataque a modems de internet. Os provedores instalam uma senha padrão e o usuário leigo permite. Mas, muitas vezes, trocar a senha não é suficiente, por causa de vulnerabilidades no firmware de alguns modems. O criminoso consegue remotamente alterar as configurações de DNS do modem e todo o tráfego de internet dos computadores pode ser monitorado. O conforto que as "coisas" proporcionam, se não estiverem protegidas, pode se transformar em transtorno e até risco de morte.

## F: As previsões indicam que, em 2020, o mundo terá 50 bilhões de equipamentos conectados, que necessitarão de infraestrutura, políticas públicas e regulamentação, mas, acima

**de tudo, segurança que garanta a privacidade dos dados. Quais os desafios nesse sentido?**

**G.R.:** A cibersegurança é um mercado interminável. Muitas empresas e usuários no Brasil ainda utilizam sistemas operacionais antigos, como o Windows XP, que não contam mais com suporte, ou piratas. Isso aumenta a exposição a ataques, com hackers explorando as vantagens de sistemas operacionais desatualizados. O maior crescimento é das ameaças que se utilizam de vulnerabilidades do dia zero (falhas no código fonte da aplicação que são desconhecidas pelos fabricantes dos softwares), e o risco financeiro está entre os mais impactantes. As empresas que não estiverem protegidas adequadamente amargarão perdas que incluem, dentre outras, o vazamento de informações. O ransomware, combinado com as vulnerabilidades da internet das coisas, continuará sendo o maior impacto financeiro nas empresas.

**F: Um relatório recente da Kasperksy Lab aponta que 29% das pessoas não fazem ideia de como um malware infectou os seus dispositivos. O que fazer para que a conscientização em torno da segurança on-line seja maior?**

**G.R.:** O conhecimento sobre os prejuízos causados a outras pessoas e empresas, por meio de notícias, pode ser o maior motivador para que elas se protejam imediatamente. A educação, às vezes, passa pelo setor jurídico das empresas, que deve mostrar as responsabilidades dos gestores e as consequências pelo descumprimento dos deveres de implantação e observância de políticas e normas.

**F: Como é o processo de desenvolvimento de produtos de segurança? O que é considerado? Qual o tempo médio de conclusão de um produto?**

**G.R.:** Na minha visão, não é suficiente ter "pronto" um bom antimalware. É preciso ter uma visão holística sobre todos os aspectos de um sistema. É importante poder gerenciar, de forma amigável, o conjunto da solução. A partir daí, estou certo que a primeira etapa é saber identificar e vir a conhecer o malware. Com uma equipe experiente, desenvolve-se a vacina, que é testada e disponibilizada para os clientes em minutos. Quando falamos em produto de segurança, ele não se conclui, mas se complementa cada vez que um novo malware é descoberto – o que acontece diversas vezes, todos os dias.

**F: O ransomware tem feito estragos em empresas e usuários ao redor do mundo, além de alimentar o cibercrime. Vale a pena pagar o resgate que é cobrado para que os arquivos sejam devolvidos, por meio de bitcoins? Qual a garantia que se tem de que os dados sequestrados serão devolvidos?**

**G.R.:** Não há garantia de resgate. Temos de nos lembrar de que estamos tratando com criminosos. Virtuais, o que é ainda pior, mas criminosos. Ransomware é mais do que um malware, passou a ser um negócio rentável. Muitos criminosos deixaram de trabalhar com outros tipos de malware para se dedicar exclusivamente ao ransomware. Alguns são destrutivos e, mesmo que o cibercriminoso in-

*Adoção de cuidados nos ambientes pessoal e profissional ajuda a intensificar a segurança das informações*

forme que devolverá o arquivo, pode ser mentira. Se você pagar ao cibercriminoso, ele, percebendo sua fragilidade, poderá tanto pedir mais dinheiro, como poderá repetir a dose e sequestrar novamente seus dados. Empresas de antivírus desenvolvem ferramentas de descriptografia. A campanha nomoreransomware.org é um exemplo disso. Alguns ransomwares podem ser descriptografados, mas há outros que não. O melhor a se fazer é utilizar proteções de endpoints que atuam preventivamente e impedem que o ransomware entre e seja instalado em qualquer computador ou dispositivo de sua rede.

**F: Qual o panorama atual dessa ameaça no Brasil?**

**G.R.:** Cibercriminosos brasileiros também desenvolvem ransomware. O XPan, que atacou hospitais, e o Notificação, podem ser decifrados, mas chegará o dia em que os criminosos brasileiros conseguirão produzir ransomwares nos quais onde a descriptografia dos arquivos não será possível.

**F: Para as grandes corporações, quais as orientações de proteção?**

**G.R.:** Existem proteções para ataques de todos os tipos. As empresas devem se proteger contra vírus, bots, trojans, worms, spyware, rookit, ransomware e backdoor, dentre outras ameaças, visíveis e invisíveis. A indústria de antivírus responde a esses ataques com a ajuda de inteligência artificial, análises estatísticas e novos métodos de detecção, como heurística. Mas o usuário deve usar um sistema operacional atualizado, assim como os demais aplicativos e o antivírus, e sempre verificar a procedência de e-mails e links antes de abri-los.

**F: Podemos dizer que os antivírus ainda são importantes para os usuários comuns ou são recomendadas outras proteções?**

**G.R.:** Claro que vírus ainda existem e causam danos, às vezes, irreparáveis. Todo usuário deve ter antivírus em seus dispositivos. Mas eles não são mais suficientes para protegerem nenhum tipo de usuário, incluindo os domésticos. São recomendados recursos como firewall pessoal, antiphishing, proteção contra roubo de senhas.

**F: Na sua opinião, por que muitas pessoas e empresas ainda são vítimas de crimes considerados "bobos"? No que elas ainda pecam?**

> ***"Todo usuário deve ter antivírus em seus dispositivos. Mas eles não são mais suficientes para protegerem nenhum tipo de usuário"***

**G.R.:** Excesso de confiança, ou melhor, falta de consciência. Além de utilizarem uma excelente proteção do endpoint, precisam ter comportamento adequado, como desconfiar de links recebidos para preenchimento de senhas.

**F: Aconselhar as empresas a trabalharem com inteligência de ameaça como forma de proteção dos próprios dados tem sido propagado. No que consiste essa forma de segurança?**

**G.R.:** Inteligência de ameaças diz respeito a como você pode se manter informado sobre as ameaças mais recentes e que surgem, constantemente, direcionadas às empresas. E se o seu sistema de SIEM (gerenciamento e correlação de eventos de segurança – em inglês, Security Information and Event Management) não possuir funcionalidades adequadas de detecção de ameaças virtuais, como você pode ser notificado a tempo sobre a maioria das ameaças persistentes avançadas perigosas? Podem ser complementados alguns serviços de inteligência de ameaças criados para atenuar esses riscos. Feeds de dados de ameaças, melhorando a solução de SIEM e aprimorando as funcionalidades de perícia usando os dados de ameaças virtuais. Relatórios de inteligência de APTs (ameaças persistentes avançadas), obtendo acesso exclusivo e proativo a descrições de campanhas de espionagem virtual de grande visibilidade, incluindo Indicadores de Comprometimento (IOC – Indicators of Compromise).

Outros itens formam um conjunto de características de uma proteção aprimorada: a fusão de inteligência de ameaças com aprendizado de máquina e a experiência de equipes de segurança de alto nível, a detecção das ameaças virtuais por algoritmos baseados em toda informação big data, plataforma global de inteligência de ameaças com base na nuvem; o processamento de metadados enviados voluntariamente por milhões de usuários para os laboratórios, enquanto os especialistas em segurança adaptam continuamente os modelos matemáticos para detectar novas ameaças sofisticadas.

Banco de imagens - Freepik

# Marco Civil da Internet: desafios a serem superados

Considerado uma das legislações mais avançadas do mundo na regulação da internet e na garantia da neutralidade da rede, o documento ainda precisa esclarecer sobre os critérios de aplicação de sanções pelo descumprimento das disposições legais

O uso da internet no Brasil começou a ser regulado em abril de 2014, com a sanção da lei nº 12.965, conhecida como Marco Civil da Internet (MCI). Considerado uma das legislações mais avançadas do mundo na regulação da internet e na garantia da neutralidade da rede, o documento trata de princípios, garantias, direitos e deveres de quem usa a rede e determina diretrizes para a atuação do Estado.

Para sustentar os direitos individuais no ciberespaço, o MCI é orientado por três princípios básicos: a neutralidade da rede, a privacidade na web e a liberdade de expressão *(veja mais na página 17)*. Considerado a Constituição Digital brasileira, o Marco Civil estabelece, como fundamentos do uso da internet, o reconhecimento da escala mundial da rede, o pluralismo, a diversidade, a abertura e a colaboração. Direitos econômicos como livre iniciativa, livre concorrência e defesa do consumidor também são encorajados desde que não conflitem com os demais princípios estabelecidos pela lei.

Embora o Marco esteja em vigor há três anos e meio, vários desafios ainda precisam ser superados. "A problematização ante a falta de normas reguladoras eficazes para a garantia dos direitos fundamentais dos usuários está longe de ser resolvida. Ela se evidencia em decorrência da falta de zelo, de efetividade e de comprometimento dos legisladores na criação e no desenvolvimento da lei nº 12.965/2014, inclusive no que diz respeito à ausência de medidas sancionadoras rigorosas e fiscalização das empresas para que garantam aos usuários um serviço qualificado, moderno e eficiente", afirma o advogado **Luiz Fernando Marra**, da Moisés Freire Advocacia, especialista em Direito Tributário.

Bruno Soares

## *HISTÓRIA*

O texto da lei nº 12.965/2014 resultou em discussões e debates iniciados em 2009. Naquele ano, havia 26 propostas no Congresso Nacional para regulamentação da internet. Uma das mais polêmicas era o projeto de lei (PL) 84/1999, que previa a destruição de dados eletrônicos de terceiros, o acesso e a obtenção de informações em sistemas restritos sem autorização e a transferência não autorizada de dados ou informações particulares, que se tornariam crime, passíveis de prisão e multa.

A reação da sociedade civil contrária a essa proposta levou a Secretaria de Assuntos Legislativos do Ministério da Justiça a realizar consultas públicas on-line para elaboração de uma lei. O debate foi efetivado a partir de um blog criado na plataforma Cultura Digital, ligada ao Ministério da Cultura. O projeto foi lançado em outubro de 2009 e dividido em duas etapas. A primeira fase, de 29 de outubro a 17 de dezembro, consistiu em uma consulta pública sobre um conjunto de princípios normativos considerados relevantes pelo governo. Após a etapa inicial, e com o seu resultado, foi elaborado um segundo documento, dividido em capítulos e artigos, já no formato de um anteprojeto de lei. Na segunda consulta pública, a discussão foi mais específica, a partir de cada um dos artigos e parágrafos do projeto.

Uma das primeiras experiências do gênero no contexto brasileiro e mundial, a consulta pública sobre o Marco Civil foi considerada uma das mais bem-sucedidas, pelo formato colaborativo e pela forma como conseguiu envolver diferentes setores da sociedade e do governo. O projeto de lei foi encaminhado ao Congresso Nacional em agosto de 2011. O Legislativo realizou nova consulta, além de audiências e seminários presenciais em 2012. Em setembro de 2013, após as denúncias de espionagem contra o governo brasileiro, realizadas pela agência de segurança dos Estados Unidos (National Security Agency – NSA) e vazadas por Edward Snowden, o poder Executivo solicitou que o projeto fosse apreciado em regime de urgência.

O Marco Civil da Internet, então, foi aprovado na Câmara dos Deputados, em março de 2014, e no Senado, em abril do mesmo ano. Foi sancionado pela Presidência da República no mesmo mês, durante o NetMundial, encontro internacional que reuniu 85 países em São Paulo e discutiu propostas para uma governança mundial da internet.

Ele, no entanto, ressalta que a criação do MCI "foi importante por colocar o Brasil entre os 10 primeiros países a instituir uma legislação regulamentadora da internet". Contudo, o jurista ressalta que não ficaram claros os critérios de aplicação de sanções pelo descumprimento das disposições legais. "Apesar de trazer diversas diretrizes referentes aos padrões de segurança no armazenamento e tratamento de dados pessoais e comunicações privadas, o decreto não determina o grau de obrigatoriedade de cumprimento das normas pelas empresas de telecomunicação digital", diz.

A falta de efetividade e de clareza nas regras sobre a liberalidade de uso e de acesso dos usuários aos serviços de internet é uma das dificuldades para que o Marco Civil cumpra seus objetivos, na avaliação do professor-adjunto de Direito Internacional da Faculdade de Direito da Universidade Federal de Minas Gerais (UFMG), **Fabrício Bertini Pasquot Polido**. "Não há disposições que regulam acerca da privacidade e da segurança na prestação de informações pessoais para realizar atividades cotidianas, como acessar contas bancárias e comprar mercadorias".

Fabrício, que também é membro do Conselho Científico e fundador do Instituto de Referência em Internet e Sociedade (Iris), esclarece que a promulgação do decreto nº 8.771, em 2016, normatizou as disposições previstas no MCI. "Nele, ficaram estabelecidas medidas relativas à neutralidade de rede, à proteção de acessos a dados pessoais e comunicações privadas, bem como à atribuição de competências para fiscalização do cumprimento das regras estabelecidas".

Para ele, ainda é cedo para discutir os efeitos da aplicação do Marco Civil no Brasil. "Os tribunais têm sido gradativamente levados a firmar entendimento jurisprudencial sobre as regras e princípios estabelecidos pela nova lei, em novo contexto social".

Arquivo pessoal

## Inclusão digital

O estímulo à inclusão digital muitas vezes acaba sendo limitado por questões econômicas e tecnológicas. Isso porque várias regiões do país não têm acesso à internet, além de empresas prestadoras de serviços digitais exigirem alto custo por uma tecnologia, por vezes, arcaica, oferecida ao consumidor. "Se o acesso à internet é limitado tecnicamente ou sofre discriminações de qualidade e quantidade, por conduta de empresas provedoras de acesso, maiores serão os efeitos constritivos sobre aqueles direitos e garantias que o Marco Civil propõe proteger", observa Fabrício.

### *COMITÊ GESTOR DA INTERNET NO BRASIL - CGI.br*

O Comitê Gestor da Internet no Brasil foi criado em 1995, pela portaria interministerial nº 147, para estabelecer as diretrizes estratégicas para o uso e desenvolvimento da internet no Brasil e para a execução do registro de nomes de domínio, alocação de endereço IP (Internet Protocol) e administração pertinente ao domínio de primeiro nível ".br". O órgão também promove estudos, recomenda procedimentos para a segurança da internet e propõe programas de pesquisa e desenvolvimento que permitam a manutenção do nível de qualidade técnica e inovação no uso da internet.

Integram o CGI.br nove representantes do setor governamental, quatro do setor empresarial, quatro do terceiro setor, três da comunidade científica e tecnológica e um representante de notório saber em assuntos de internet. A atual composição do Comitê foi estabelecida pelo decreto nº 4.829, de 3 de setembro de 2003, da Presidência da República.

## *MARCO CIVIL DA INTERNET*

### PRINCÍPIOS BÁSICOS

**Neutralidade na rede** – a rede deve ser igual para todos, sem diferença quanto ao tipo de uso. O usuário poderá acessar o que quiser, independentemente do tipo de conteúdo, pagando de acordo com o volume e a velocidade contratados. O MCI prevê que a neutralidade será regulamentada por meio de decreto após consulta ao Comitê Gestor da Internet no Brasil e à Agência Nacional de Telecomunicações.

**Privacidade na web** – somente por meio de ordens judiciais, para fins de investigação criminal, será possível ter acesso à privacidade, à inviolabilidade e ao sigilo das comunicações dos usuários pela internet. Os provedores de conexão são proibidos de guardar os registros de acesso a aplicações de internet. Toda provedora de aplicação, sendo empresa constituída juridicamente no Brasil, deverá manter o registro – o rastro digital dos usuários em sites, blogs, fóruns e redes sociais – por seis meses. Essas informações poderão ser utilizadas durante esse período, desde que com autorização prévia do usuário.

**Liberdade de expressão** – as aplicações e os provedores de acesso não serão mais responsabilizados pelas postagens de seus usuários e as publicações só poderão ser retiradas do ar mediante ordem judicial. As empresas só serão responsabilizadas por danos gerados por usuários se não acatarem a decisão da justiça. O MCI assegura ainda a proteção a dados pessoais e a registros de conexão. As empresas que descumprirem as regras poderão ser penalizadas com advertência, multa, suspensão e proibição definitiva de suas atividades, com possibilidade de penalidades administrativas, cíveis e criminais.

## *GOVERNANÇA E USO DA INTERNET NO BRASIL - FUNDAMENTOS*

1) Liberdade, privacidade e direitos humanos
2) Governança democrática e colaborativa
3) Universalidade
4) Diversidade
5) Inovação
6) Neutralidade da rede
7) Inimputabilidade da rede
8) Funcionalidade, segurança e estabilidade
9) Padronização e interoperabilidade
10) Ambiente legal e regulatório

A efetiva proteção de dados pessoais na web é outra questão desafiadora, já que os usuários fornecem diversas informações às empresas prestadoras do serviço. "No Marco Civil, não há um detalhamento acerca do tema, que acarreta a criação de uma nova norma para regulamentar amplamente a matéria. Isso é imprescindível para coibir o uso indevido de elementos individuais em atividades criminosas e a elevada exposição da intimidade dos consumidores", comenta Marra.

Ele também defende a redução do conflito entre o Poder Judiciário e as empresas de tecnologia e comunicação para que o Marco Civil atinja sua finalidade. "Um exemplo de impasse entre os setores citados é o bloqueio de aplicativos, como o WhatsApp, por decisão judicial, o que pode causar insegurança aos usuários". *(Leia mais sobre WhatsApp na página 51).*

Já Fabrício ressalta a importância de alcançar a consistência interpretativa sobre os consensos já estabelecidos no Direito de Internet. "É justamente isso que se apresenta problemático no Brasil. Juízes e legisladores brasileiros captam mais facilmente a realidade dos cartórios, dos papéis e dos códigos que a dos espaços de transformação, participação e interação na rica sociedade global do conhecimento".

A expectativa é que o debate sobre o Marco Civil da Internet continue nos próximos anos. Comissões do Congresso Federal e do Senado estão discutindo vários projetos para resolução de problemáticas relacionadas à efetividade e à segurança na prestação dos serviços de acesso à internet. Grande parte das propostas refere-se à regulamentação da suspensão e do bloqueio dos aplicativos e ainda da franquia e dos limites de uso da internet particular. "Diante da relevância desse assunto, espera-se que o Marco Civil da Internet continue sendo discutido e aplicado com coesão, eficiência e técnica, atentando-se aos fundamentos e princípios previstos na lei nº 12.965", considera Marra.

# Guardiã de informações

A informação é um ativo muito importante para qualquer tipo de organização, tanto privada quanto pública. Por isso, com a crescente evolução e a sofisticação dos ataques cibernéticos, os investimentos em Tecnologias de Informação e Comunicação (TICs) tornaram-se ainda mais necessários, já que os sistemas dão apoio não só à execução das atividades, como também são estratégicos para a manutenção do próprio negócio.

Na Prodemge, essa realidade não é diferente. Afinal, além de zelar pela segurança da rede corporativa e dos sistemas que hospedam as informações dos inúmeros clientes, em sua maioria órgãos públicos mineiros, a empresa também monitora e notifica as invasões contra sites identificados pelo domínio mg.gov.br e que não são órgãos do Estado, como ocorre com prefeituras e câmaras municipais. "Mesmo sendo órgãos da esfera municipal, o mg.gov.br é um domínio de responsabilidade da Prodemge, por isso é também função dela informar os incidentes aos gestores desses sites", afirma o gerente **Bruno Moreira Camargos Belo**, da Gerência de Tratamento de Incidentes e Operações de Segurança da Companhia ou Centro de Tratamento de Incidentes de Operações de Segurança (CTIS), como é conhecida externamente.

Criada em fevereiro de 2013, essa é a área responsável por monitorar, identificar e tratar os incidentes de segurança que ocorrem contra a rede corporativa do governo de Minas, seus sistemas e os sistemas de seus clientes.

No local, uma equipe trabalha focada em registrar, tratar, monitorar e rastrear as tentativas de invasões. "O objetivo do CTIS é detectar e corrigir qualquer tipo de vulnerabilidade existente e também identificar e tratar os incidentes quando ocorrem, para que o sistema ou serviço afetado seja restabelecido o mais rápido possível. Caso o ataque ocorra fora do horário do expediente, o próprio Centro possui tecnologia suficiente para gerar, automaticamente, alertas de ataques para acionar imediatamente a equipe".

Embora não seja possível precisar o tempo médio gasto pela Prodemge para reparar um incidente de segurança, "pois cada caso depende de uma série de variáveis", como explica Bruno, as respostas são bem rápidas. "Prezamos por essa agilidade, já que a indisponibilidade de um sistema ou serviço, mesmo que por um curto espaço de tempo, pode comprometer o negócio de uma instituição, caso ela não trate o incidente de forma rápida e eficiente", complementa.

Arquivo pessoal

As motivações dos hackers para invadir os sistemas públicos são as mais diversas. Entre elas estão as tentativas de roubo de informações, de tornar sistemas e serviços indisponíveis ou até mesmo desfigurar o conteúdo de sites, como forma de protesto. "Em épocas de maior visibilidade, como ocorrido na Copa do Mundo e em eleições, por exemplo, observamos algumas tentativas de manifestos", lembra.

No caso específico da Prodemge, as ocorrências mais comuns de ataque são o DDoS, sigla para Distributed Denial of Service, e o cross site scripting. O primeiro consiste num ataque para tornar alguma infraestrutura ou sistema indisponível. "Uma vez identificada essa tentativa, o próprio CTIS consegue bloqueá-lo, automaticamente", explica Bruno.

Já por meio do cross site scripting, o hacker injeta um arquivo no site com o intuito de mudar seu conteúdo ou até mesmo ter acesso a um servidor. "Em um cenário em que os ataques estão evoluindo de maneira muito rápida, malwares cada vez mais sofisticados estão aparecendo. Felizmente, não temos registros de perda de informação na Prodemge como consequência de um ataque cibernético", afirma.

### *ESTRATÉGIA DE GUERRA*

A Prodemge adota uma estratégia referenciada como Defesa em Profundidade, definida como um conjunto de soluções tecnológicas implementadas em várias camadas virtuais de segurança para impedir o sucesso de um ataque e, consequentemente, a corrupção dos sistemas e dados. "É uma estratégia muito antiga, baseada na tática de guerra, onde os vários recursos disponibilizados em camadas são utilizados para impedir o ataque", explica Bruno.

Os recursos mais comuns implantados nelas são os firewalls de rede, de aplicação (WAF) e de host, estes últimos usados para proteger servidores, aplicações e sistemas; os IPS (Intrusion Prevention Systems), sistemas de prevenção de intrusão; os sistemas anti-DDoS, para ataques de negação de serviços com atuação no tráfego de rede; IDS Host, sistemas de detecção de intrusão em servidores; patchs de segurança e antivírus para a proteção das estações de trabalho.

# Serviços públicos protegidos

Assim como a Prodemge tem papel fundamental no cenário da cibersegurança da esfera pública mineira, o Governo Federal também zela pelas redes e sistemas de órgãos que hospedam os dados que sustentam os serviços básicos de um país, como energia, telecomunicações, transporte, defesa, dentre outros.

Desde 2003, os investimentos para conter os ataques cibernéticos já fazem parte da rotina do Governo Federal. Naquele ano, foi criado o Centro de Tratamento de Incidentes de Redes do Governo (CTIR Gov). Vinculado ao Gabinete de Segurança Institucional (GSI) e pertencente ao Departamento de Segurança da Informação e Comunicações (DSIC), ele é responsável pelo tratamento e registro de incidentes de segurança nas redes de computadores dos órgãos públicos brasileiros, em funcionamento no território nacional e no exterior.

O vírus WannaCry, propagado em maio de 2017 e responsável por afetar mais de 200 mil máquinas em todo o mundo, atingiu poucos órgãos públicos brasileiros, recorda o diretor do DSIC, **Arthur Pereira Sabbat**. "Os únicos incidentes registrados se deram em função do desligamento da rede de alguns setores, situação que foi revertida no mesmo dia do ocorrido". Também naquele mesmo dia, o CTIR Gov emitiu alertas com as orientações de mitigação da ameaça.

Enviados a todos os órgãos, esses alertas trataram das vulnerabilidades ou dos incidentes cibernéticos que poderiam apresentar mais danos tecnológicos ao governo. Com base nesses alertas, o CTIR Gov ainda emite, desde 2011, relatórios trimestrais e anuais com as estatísticas dos incidentes mais comuns nas redes computacionais do governo.

Arquivo pessoal

Além disso, em julho de 2017, foi formada uma equipe para traçar um diagnóstico da Tecnologia da Informação e Comunicação (TIC) e da segurança da informação. Composta por colaboradores do GSI e do Ministério do Planejamento, Desenvolvimento e Gestão (MPDG), o grupo realizou visitas a 30 órgãos do Governo Federal entre julho e setembro de 2017. "Esses encontros foram excelentes oportunidades para encontrarmos soluções que apoiem a gestão segura dos ativos de informações desses órgãos", comenta Sabbat.

Durante as visitas, foram aplicados questionários para identificar o panorama nacional da cibersegurança. Os dados gerados ainda estão sendo apurados. No entanto,

Sabbat ressalta que ficou evidente que o cenário brasileiro está muito avançado quando comparado ao de outros países. "Os ataques cibernéticos têm impacto muito maior lá fora. Felizmente, no Brasil, eles não têm feito tantas vítimas. E isso é resultado de uma melhora crescente na cultura de segurança da informação e cibernética dos cidadãos", elogia.

## Política

Em fevereiro, também foi instituído pelo GSI um grupo de trabalho específico, formado por representantes de 11 ministérios, para discutir os aspectos de segurança cibernética, com o intuito de criar a Política Nacional de Segurança da Informação (PNSI). "As crescentes ameaças cibernéticas e a complexidade na gestão dos ativos de informação, somadas às transformações digitais dos serviços prestados pelo governo e a disseminação de dispositivos de internet das coisas, motivaram a idealização dessa política", informa Sabbat.

Ainda segundo ele, a PNSI será um importante instrumento político e estratégico e trará benefícios para toda a população. "Por meio dela, o cidadão irá dispor de serviços públicos cada vez mais confiáveis e resilientes, uma vez que os órgãos e as entidades conseguirão aprimorar os níveis de segurança da informação mediante a aplicação dos conceitos determinados pela política".

Sabbat também informa que a política não tem previsão para entrar em vigor. "A PNSI compõe um processo administrativo que passará por algumas fases e apreciações, além da apreciação jurídica pela Casa Civil", explica. Dentre os assuntos abordados pelo documento, estão os mecanismos para proteção e sigilo das informações armazenadas, processadas e veiculadas; o interesse da privacidade e da segurança de pessoas físicas e jurídicas; a proteção do capital intelectual, científico e tecnológico; o aprimoramento jurídico para implementação da segurança da informação; a investigação e a prevenção da quebra dos mecanismos de proteção e tratamento dos dados comprometidos.

O último relatório emitido pelo CTIR, no qual foram analisados os incidentes registrados nos meses de abril, maio e junho de 2017, mostrou que o número de malwares caiu em 43% quando comparado ao trimestre anterior. Sobre o ransomware, software também nocivo, já que restringe o acesso ao sistema infectado e cobra um resgate para que ele seja restabelecido, Sabbat conta que o governo nunca pagou pelo resgate de informações sequestradas dos órgãos. "Tal pagamento nunca será a garantia de liberação dos dados. Por isso, reforçamos sempre a importância da atividade de backup frequente dos sistemas", finaliza.

# Panorama energético em tempo real

O uso da energia elétrica faz parte da vida moderna e está presente em diversas atividades diárias, seja em casa, seja no trabalho, de Norte a Sul. E, para garantir que não falte energia em nenhum canto do país, foi criado, em 1998, o Operador Nacional do Sistema Elétrico (ONS). Coordenado pela Agência Nacional de Energia Elétrica (Aneel), ele controla e coordena a geração e a transmissão de energia elétrica por meio do Sistema Interligado Nacional (SIN), que corresponde, atualmente, a 96,6% da energia elétrica produzida no Brasil.

Para controlar o SIN, o órgão conta com quatro centros de operação regionais. Em funcionamento 365 dias por ano, durante 24 horas, eles estão localizados no Rio de Janeiro (RJ), Recife (PE), Florianópolis (SC) e Brasília (DF), respondendo, respectivamente, pelas regionais Sudeste, Nordeste, Sul, sendo que a capital

Divulgação ONS

*Centro de operação regional do ONS em Recife*


Divulgação ONS

*Centros de operações regionais controlam o Sistema Interligado Nacional (SIN)*

federal, também chamada de Central, acumula a região Centro-Oeste.

"Cada uma das regionais gera dados fundamentais para que o ONS enxergue o panorama energético do país em tempo real", explica o especialista João Roberto de Castilho Maksoud. Por meio dessas informações, armazenadas na rede operativa do órgão, ele orienta as empresas de geração, transmissão e distribuição de todo o país.

A telecomunicação entre elas e o ONS é feita por meio de dois servidores, para garantir a redundância dos processos, "já que na ausência de um, o outro assume a função", explica João. Além de assegurar o fornecimento de energia elétrica para todo o país, outra preocupação do ONS é proteger os dados gerados pelos centros. "Prevenir as ameaças cibernéticas garante não só a disponibilidade de energia ao cidadão, como também a integridade e a confiabilidade dela", complementa o analista de TI Geraldo Carlos Wosny Oliva da Fonseca, do ONS.

Os quatro centros geram, em média, 4 mil medidas por segundo. Essas medidas incluem informações sobre equipamentos, cargas e capacidade de todas as empresas de geração, transmissão e distribuição controladas. "A indisponibilidade de qualquer tipo de dado pode comprometer o controle das operações, pois não permite que o ONS tenha uma visão do todo", afirma João.

Por isso, com o intuito de zelar pela integridade dos centros, o ONS utiliza firewalls, IPSs, soluções antimalware, filtros de conteúdo, além do monitoramento dos incidentes registrados. No entanto, João destaca que, embora os investimentos em infraestrutura e segurança sejam importantes, a correta conduta dos colaboradores também faz toda a diferença. "A linha de defesa mais importante está em cada um de nós. Todos nós fazemos parte da proteção", frisa.

Tanto é que o ONS possui uma política própria de uso e segurança da informação, contendo orientações às condutas dos colaboradores. "Esse documento é uma forma de reforçar o compromisso do órgão com a proteção das informações de sua propriedade ou sob sua guarda, bem como com o uso adequado e consciente dos ativos de informação disponíveis", finaliza Geraldo.

## *INFORMATIZAÇÃO DOS PROCESSOS DE TELEFONIA*

Investimentos para manter a segurança das informações também fazem parte da rotina da Agência Nacional de Telecomunicações (Anatel), responsável pela regulação do setor de telefonia fixa e de celular e que também conta com um canal específico de atendimento ao público. Batizado de Serviço de Informação ao Cidadão (SIC) e regulamentado pela lei nº 12.527/2011, ele permite que qualquer pessoa, física ou jurídica, possa encaminhar os pedidos e acompanhar os prazos e as respostas às solicitações feitas pela Anatel.

Um importante marco, ocorrido em novembro de 2015, foi a informatização de todos os processos realizados pela agência. Além de trazer mais agilidade e confiabilidade, essa mudança marcou a substituição do uso do papel pelo Sistema Eletrônico de Informações (SEI), responsável pelo armazenamento das informações geridas pela Anatel.

Porém, dois anos antes do início do funcionamento do SEI, em 2013, a agência já havia criado a Política de Segurança da Informação e Comunicações (Posic). O documento estabeleceu diretrizes para a segurança do manuseio, tratamento, controle e proteção dos dados, informações e conhecimentos produzidos, armazenados ou transmitidos por ela.

Também naquele ano foi formada uma equipe própria para tratar de incidentes de segurança de informação. Mensalmente, a média é de 23 ocorrências. Desse total, a maioria é considerada de baixo potencial de risco.

Porém, já houve incidentes de maior potencial ofensivo, informa o órgão, por meio de sua assessoria de comunicação. Dentre os mais marcantes, estavam ataques que tentaram indisponibilizar os serviços, extrair/alterar dados da rede e enviar mensagens com o intuito de instalar programas maliciosos na rede (fishing).


Sinclair Maia

*Em 2015, a Anatel informatizou os processos realizados pela agência*

# Segurança nas eleições, democracia garantida

Em uma democracia, votar é um ato de cidadania e é na urna que o cidadão tem a oportunidade de escolher os governantes que fazem e executam as leis que interferirão diretamente no cotidiano. Por mais uma vez, em outubro de 2018, ocorrerão as eleições gerais, quando serão selecionados o presidente, os governadores, os senadores e os deputados federais e estaduais.

Dada a importância e a complexidade das eleições, o Tribunal Superior Eleitoral (TSE), instância jurídica máxima da Justiça Eleitoral brasileira, tem investido continuamente em tecnologias que assegurem a confiabilidade de todos os processos. É o que ressalta o secretário de Tecnologia da Informação do TSE, **Giuseppe Janino**. "Desde o surgimento da urna eletrônica, em 1996, as equipes estão sempre se reciclando e buscando inovações tecnológicas para que tragam mais melhorias à segurança".

Para garantir a idoneidade dos processos eleitorais, Giuseppe conta que todas as ferramentas tecnológicas utilizadas são próprias, desenvolvidas e controladas pelo TSE. Como exemplo, ele cita os firmwares, definidos como um conjunto de instruções operacionais programadas diretamente no hardware de um equipamento eletrônico, assim como a utilização de um sistema operacional próprio. Chamado Uenux, ele é baseado no Linux, mas foi idealizado por colaboradores da Secretaria de Tecnologia da Informação do TSE.

Fora as ferramentas tecnológicas autorais, as urnas também recebem cuidados especiais. Apenas os softwares próprios são passíveis de serem executados por elas. "Para que rodem nas urnas, é preciso que sejam assinados digitalmente pela Justiça Eleitoral, processo que é garantido por uma infraestrutura de chaves públicas dedicada a essa finalidade", conta Giuseppe.

A partir dessa assinatura, é gerado um certificado digital, documento que comprova a autoria do TSE. Feito isso, membros dos partidos políticos, do Ministério Público (MP) e da Ordem dos Advogados do Brasil (OAB) também o assinam digitalmente. "Juntas, essas assinaturas geram códigos-fonte que são armazenados em uma sala-cofre do TSE, com o intuito de prezar pela idoneidade dos processos", complementa.

Mais do que investimentos no aparato tecnológico, a equipe do TSE também coordena testes junto aos colaboradores dos Tribunais Regionais Eleitorais (TREs), com o intuito de validar e homologar os sistemas utilizados. Uma avaliação específica para verificar a segurança deles, intitulada Teste Público de Segurança do Sistema Eletrônico de Votação, também é realizada no ano anterior à eleição, para identificar possíveis falhas e vulnerabilidades relacionadas à violação da integridade ou do anonimato dos votos. É um momento precioso para identificar oportunidades de melhorias, uma vez que especialistas de tecnologia de todo o país participam desse processo", complementa Giuseppe.

Roberto Jayme

## Votação paralela

Outro mecanismo criado pela Justiça Eleitoral para comprovar a confiabilidade do sistema eletrônico é a votação paralela. O procedimento, embasado pela resolução do Tribunal Superior Eleitoral (TSE) nº 23.397/2013, ocorre no mesmo dia e horário das eleições e conta com a participação do MP, da OAB e de representantes dos partidos políticos, além de ser aberta à imprensa e à sociedade civil.

As urnas utilizadas na votação paralela são escolhidas na véspera da eleição, por meio de sorteio feito pelos TREs de cada estado. Em seguida, os equipamentos são retirados dos seus locais de origem e levados para as sedes dos tribunais regionais, onde permanecem sob vigilância.

Nelson Júnior

*Novo modelo de urna será utilizado nas eleições 2018*

Os juízes eleitorais das zonas que terão as urnas sorteadas são comunicados pelos magistrados dos TREs responsáveis pelos sorteios, para que possam substituir os equipamentos por outros do estoque de reserva. No mesmo dia e horário da votação oficial, depois que os fiscais dos partidos e representantes das coligações verificam a assinatura e o resumo digital dos sistemas eleitorais, é autorizado o início da votação paralela. Esses fiscais votam em cédulas de papel, que são armazenadas em urnas de lona.

Os candidatos a serem votados, previamente estabelecidos e de conhecimento de todos os presentes, deverão constar na urna eletrônica. A urna de lona é aberta e os votos são retirados, um a um, lidos e digitados em um microcomputador, em que é instalado o sistema de apoio à votação paralela. O sistema imprime duas vias de cada voto. Uma via é anexada à cédula em papel, e a outra é utilizada para a votação na urna eletrônica.

Nesse momento, quem vota na urna eletrônica deve permitir a filmagem da via impressa pelo sistema de vídeo e ler em voz alta o conteúdo da cédula ao mesmo tempo em que digita os dados no equipamento. A votação paralela se encerra às 17h, mesmo horário do fim do pleito oficial. O sistema então imprime relatórios contendo comparativos com o sistema de votação paralela, para aferição dos resultados. Os dados impressos no boletim das urnas eletrônicas utilizadas na votação paralela são comparados com os da lista de votação, a fim de conferir se o que foi digitado na urna eletrônica está idêntico aos votos das cédulas de papel.

"Qualquer pessoa consegue verificar se o que foi votado é aquilo que saiu", explica o coordenador de Sistemas Eleitorais do TSE, José de Melo Cruz. Ele ressalta que "essa é uma cerimônia que deve ser acompanhada pela sociedade, pela imprensa, pelos partidos políticos, porque é uma forma de garantir a lisura do processo".

## Novidades para 2018

No próximo ano, será usado um novo modelo de urna eletrônica, criado para se adaptar ao voto impresso, em atendimento à lei nº 13.165/2015, aprovada pelo Congresso Nacional. A estimativa é de que 30 mil urnas desse novo modelo sejam empregadas em todo o país no pleito de 2018. "Apesar de a mudança ter sido motivada pela obrigatoriedade da lei que determina o voto impresso, o TSE já planejava repaginar a máquina eletrônica, que completou 20 anos em 2016", explica Giuseppe.

Com layout moderno, funcionamento em módulos acoplados e bateria com duração maior, o novo equipamento busca garantir a votação em tempo razoável, considerando que a impressão do voto em experiências anteriores foi a causa de grandes filas e aumento no tempo de votação do eleitor.

Outra vantagem destacada por Giuseppe é que o novo modelo também resultará em economia de recursos públicos. "O funcionamento em módulos permitirá que a máquina seja desmontada e ocupe espaço menor na caixa de armazenamento. Isso facilitará o transporte e, consequentemente, diminuirá a quantidade de viagens necessárias para levá-la aos postos de votação", explica.

## *PROTEÇÃO CONTRA FRAUDES*

Para que a votação ocorra de forma segura, o TSE adota uma série de procedimentos legais e administrativos antes e após o dia das eleições.

- **Cadastramento biométrico dos eleitores:** por meio dele, o TSE tem acesso às informações de todos os cidadãos. Entre as eleições, esse banco de dados é atualizado com o intuito de assegurar que cada pessoa seja única no dia da votação. O cadastro é finalizado em maio do ano eleitoral e reaberto logo após o fim das eleições.
- **Cadastramento dos partidos e candidatos:** as informações de ambos são alimentadas nos sistemas, de acordo com as regras estabelecidas. Antes e depois das eleições, as situações legais dos candidatos são averiguadas. Isso também ocorre com os partidos políticos, a cada dois anos.
- **Atualização das seções:** ao longo dos anos, com o intuito de otimizar o uso de recursos, como urnas e outros suprimentos, algumas seções são modificadas.
- **Urnas eleitorais:** a cada ciclo, é sempre avaliada a necessidade de aquisição de novas urnas e outros suprimentos indispensáveis para o uso das eleições, como bobinas, mídias de carga e de resultado, lacres, embalagens e cabinas de votação.
- **Comunicação:** durante as eleições, as informações trafegam por uma rede segura, única para todo o país, contratada e mantida pelo TSE. Essa rede conecta todos os TREs, assim como as zonas eleitorais mantidas em todo o território nacional.

# Mais de duas décadas de mudanças

Em 2018, a criação da urna eletrônica completará 22 anos no Brasil. Ela foi usada pela primeira vez em 1996, durante o pleito municipal, por mais de 32 milhões de brasileiros, o que correspondia a um terço do eleitorado da época, em mais de 57 cidades. "Podemos considerá-la como importante marco tecnológico, uma vez que, desde então, os sistemas que a compõem passaram por diversas atualizações", relembra Giuseppe.

A experiência obtida naquele ano foi fundamental para as eleições de 2000, quando foram totalmente informatizadas, uma vez que alguns componentes de software da urna passaram por atualizações para que os processos fossem ainda mais otimizados. Quatorze anos depois, a biometria foi adotada no processo eleitoral, "tecnologia que praticamente excluiu a possibilidade de intervenção humana", ressalta Giuseppe.

A leitura biométrica para identificação do eleitor foi usada pela primeira vez em 2008, em apenas três municípios: São João Batista (SC), Fátima do Sul (MS) e Colorado do Oeste (RR). "Tanto é que, depois dos bons resultados e da aceitação das pessoas, a identificação biométrica foi expandida para outros 57 municípios nas eleições ocorridas em 2010, sendo completamente empregada em 2014", informa Giuseppe.

## A URNA NA HISTÓRIA

**1994**
**Justiça eleitoral processa o resultado da eleição por via eletrônica**

**1996**
**Urna eletrônica é usada para computar votos no pleito municipal**

**2000**
**Primeira eleição totalmente informatizada no Brasil**

**2008**
**Elaborado projeto-piloto de identificação biométrica de eleitores nas urnas**

**2014**
**Biometria é utilizada em todo o país nas eleições gerais**

Fonte: TSE

# Pela sustentabilidade dos negócios

A cibersegurança tem extrapolado a área de Tecnologia da Informação e Comunicação (TIC) e se tornado, de forma crescente, um tema relevante para a sustentabilidade dos negócios de qualquer empresa. Basta relembrar as inúmeras vezes em que a palavra ransomware – código malicioso que, depois de instalado, bloqueia o acesso aos arquivos do computador e só os libera após o pagamento de resgate em moeda virtual, como o bitcoin – foi citada. Isso porque, em maio de 2017, ocorreu um dos maiores ataques cibernéticos da história.

Batizado de WannaCry, o malware atingiu o sistema Windows, comumente utilizado por organizações e usuários em todo o mundo. No total, foram afetados mais de 70 países, dentre eles o Brasil, infectando mais de 200 mil máquinas. Entre os fatores que explicam os fortes estragos causados por esse ransomware, na época, estava a combinação do malware a uma vulnerabilidade no Windows, propiciando a propagação rápida e automática na rede.

Porém, apesar do WannaCry, não é de hoje que os ataques cibernéticos tiram o sono dos usuários, principalmente, no mundo empresarial. Dados do último estudo anual da IBM em parceria com o Instituto Ponemon, *Custos de Violação de Dados*, mostram que houve aumento histórico no número de incidentes provocados e nos custos gerados com a violação de dados no Brasil. O valor total desembolsado para reparar as invasões, em 2016, foi de R$ 4,72 milhões, enquanto, em 2015, a quantia foi de R$ 4,31 milhões, o que corresponde a um aumento de 9%.

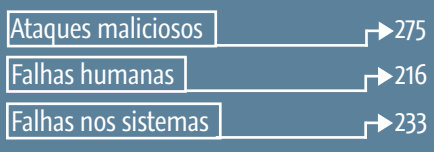
Para o gerente Bruno Moreira Camargos Belo, da Gerência de Tratamento de Incidentes e Operações de Segurança da Prodemge, área responsável pelo controle e combate aos ataques cibernéticos contra os sistemas e a rede corporativa do Governo de Minas, os investimentos em cibersegurança aumentaram de maneira exponencial. "Mergulhado em um contexto em que a evolução tecnológica é constante, a informação tem cada vez mais valor e os ataques cibernéticos se tornaram uma ameaça real até mesmo para usuários domésticos, investimentos em cibersegurança passaram a ser algo mandatório para que se consiga evitar perdas financeiras e possa manter o negócio das organizações em pleno funcionamento", afirma.

A pesquisa também mostrou que os ataques maliciosos ainda são a principal causa da violação de dados, sendo responsáveis por 44% dos casos analisados; seguidos de falhas humanas, que incluem funcionários desatentos ou negligentes que causaram 31% dos casos; e falhas nos sistemas, que representaram 25% do total.

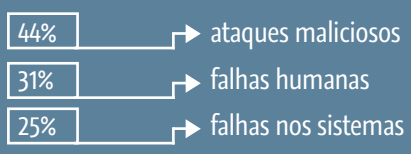
Para esse levantamento, o estudo contou com a participação de 166 organizações de 12 diferentes segmentos e tomou como base os custos de 36 empresas. As organizações mais afetadas foram aquelas voltadas para as indústrias de serviços, finanças e tecnologia.

***Custos médios per capita para reparar a violação de dados nos últimos cinco anos, em reais***


***Custo médio per capita para reparar a violação de dados, considerando as principais causas sofridas pelas empresas brasileiras, em reais, em 2016***




***Causas das violações de dados ocorridas nas empresas brasileiras***



# Reparação de dados

Ainda de acordo com a pesquisa, cada registro comprometido gera, em média, uma despesa de R$ 246 para reparação do dado. Em relação a 2016, o valor também aumentou em 9%, uma vez que, naquela época, era R$ 225.

Quanto maior o número de registros roubados, mais alto é o custo da violação de dados, explica o líder de Segurança da IBM Brasil, **João Rocha**. "Para se ter uma ideia, as companhias que tiveram vazamentos envolvendo menos de 10 mil registros tiveram um custo médio de R$ 2,07 milhões, enquanto os que tiveram 50 mil ocorrências comprometidas registraram um valor de R$ 6,73 milhões".

Outro fator que influencia o valor para reparar as violações é o tempo de identificação de invasão, pois quanto maior a agilidade em detectar e conter o malware, menores os custos arcados pela empresa. O estudo também aponta que, em média, as companhias demoraram 250 dias para registrar uma invasão e 105 para conter o vazamento de dados.

Caso o tempo de identificação fosse inferior a 100 dias, o custo médio para identificar uma violação seria de R$ 4,13 milhões. No entanto, se for superior a esse tempo, o valor subiria para R$ 5,30 milhões. "Esses dados comprovam que as empresas que não investirem em soluções de segurança, em processos internos para correção de vulnerabilidades, conscientização de usuários, identificação e resposta rápida a ataques cibernéticos terão prejuízos incalculáveis nos próximos anos", afirma Bruno.

### *Custo médio total da organização para reparar a violação dos dados nos últimos cinco anos, em milhões de reais*


### *REPUTAÇÃO COMPROMETIDA*

Além das perdas financeiras, os ataques também afetam a reputação das empresas. Em 2013, a investida sofrida pela Target, grande varejista de roupas nos Estados Unidos, culminou no vazamento de 110 milhões de números de cartões de crédito e débito, senhas e dados pessoais, por meio de um software malicioso instalado nas caixas registradoras.


Bruno Favery

# Imprudência de funcionários abre brecha na blindagem das corporações

Os programas maliciosos de fraude de informações tecnológicas estão cada dia mais sofisticados. O investimento das empresas para blindar esses ataques, no entanto, não deve ficar restrito aos especialistas da área de tecnologia. Muitos gestores não sabem, mas o risco maior de vazar informações estratégicas pode estar nos próprios funcionários. Cerca de 46% dos incidentes de segurança de tecnologia da informação (TI) são causados pelos colaboradores, segundo relatório da empresa de cibersegurança Kaspersky Lab e da analista de mercado B2B International, *O fator humano na segurança de TI: como os funcionários tornam as empresas vulneráveis de dentro para fora.*

O levantamento mostrou que os funcionários desinformados ou descuidados são uma das causas mais prováveis dos incidentes de segurança virtual. Eles só perdem para o malware. E o que é pior: os colaboradores costumam não informar o problema, pois temem ser punidos ou ficam constrangidos por serem responsáveis por algo errado. Quando eles percebem o engano, 40% preferem manter segredo, trazendo consequências mais drásticas e aumento do prejuízo. As equipes de segurança precisam ser capazes de identificar rapidamente as ameaças que enfrentam para poderem escolher a tática de atenuação correta.

Os ataques eletrônicos geram uma fragilidade que deve ser resolvida em vários níveis, não apenas pelo departamento de segurança de TI. Isso significa que a proteção dos dados eletrônicos não está apenas no âmbito da tecnologia, mas também da cultura e do treinamento da organização. E, nesse ponto, o envolvimento da diretoria e do setor de recursos humanos (RH) é fundamental. "Temos visto os grandes prejuízos que os incidentes trazem. É preciso que as empresas façam treinamento constante dos profissionais, para que estejam atualizados e reciclados", afirma **Dimitry Palma Lima Boczar**, sócio-gestor da Digicomp Engenharia e Tecnologia.

Divulgação

## Portas abertas para os hackers

Embora os hackers modernos tenham se munido de alta tecnologia para planejar um roubo, os analistas avaliam que é provável que comecem explorando o ponto de entrada mais frágil nas empresas: a natureza humana. Segundo a pesquisa da Kaspersky Lab, um terço (28%) dos ataques direcionados sobre empresas no último ano começou com e-mails fraudulentos, senhas fracas e chamadas falsas do suporte técnico. E quando não há informação suficiente disponível, é fácil os trabalhadores ignorarem algumas questões, como a perda de dispositivo eletrônico ligado à rede da empresa. "Um cartão de memória caído no parque de estacionamento ou próximo de uma secretária pode comprometer toda a rede", frisa David Jacoby, um investigador de segurança da Kaspersky Lab, em comunicado.

Um contador descuidado, por exemplo, pode facilmente abrir arquivo malicioso disfarçado como fatura de um dos inúmeros fornecedores da empresa e, assim, desligar toda a infraestrutura da organização, tornando-se cúmplice involuntário dos invasores. "As empresas têm a ferramenta de proteção. Mas, se ela não é usada de forma correta pelo funcionário, traz vulnerabilidade para o negócio", alerta Dimitry.

Segundo os especialistas, um trabalhador que esquece o celular desbloqueado no táxi, por exemplo, é tão

perigoso quanto um usuário insatisfeito que maliciosamente vaza informações para um concorrente. "As fragilidades acontecem também no momento em que os funcionários salvam ou copiam informações importantes no pendrive ou na própria máquina. Se for roubado, é um problema", observa Dimitry.

A boa notícia do levantamento da Kaspersky Lab é que as organizações estão acordando para os problemas de vulnerabilidade causados por funcionários: 52% das empresas pesquisadas admitem que suas equipes são o elo mais fraco em sua segurança de TI. E 35% das empresas buscam melhorar a segurança por meio do treinamento das equipes, sendo esse o segundo método mais popular de defesa cibernética, atrás da implementação de software mais sofisticado.

Pequenas empresas, com até 50 funcionários, se preocupam menos com violações de segurança cibernética produzidas por atividades de funcionários do que grandes corporações. Apenas 36% das pequenas empresas se preocupam com o descuido de suas equipes, enquanto mais da metade das de médio e grande portes considera isso uma questão essencial, segundo o relatório. Os autores do levantamento analisam que um dos motivos é que as "grandes empresas têm medidas de segurança mais rígidas, e dedicam-se mais à formação dos funcionários".

## Criptografia é essencial

Na avaliação de Dimitry, enquanto houver uma criptografia validada como parte da estratégia de segurança da empresa, há esperança. "É fundamental", diz. Mesmo que o funcionário não tenha tomado precauções pessoais para bloquear o telefone, por exemplo, o departamento de TI pode executar uma exclusão seletiva revogando as chaves de descriptografia usadas para os dados da corporação. Mas esse é apenas o primeiro passo que as organizações precisam para a cibersegurança, e o treinamento constante de todo o quadro pessoal não pode ficar fora desse processo.

### *OS ERROS MAIS COMUNS*

- ***Seguir um link em e-mail suspeito.***
- ***Perder o telefone celular corporativo.***
- ***Confiar em uma chamada falsa de um técnico da informática.***
- ***Senhas fracas (importante usar no mínimo oito caracteres, em letras maiúsculas e minúsculas, números e símbolos).***
- ***Visitas a sites não autorizados .***
- ***Cópia de informação estratégica da empresa em pendrive ou em máquinas pessoais.***
- ***Deixar a máquina ligada quando sair do ambiente de trabalho.***


Fonte: Kaspersky Lab e Digicomp

# Ataque traz prejuízos financeiros e na reputação

Os crimes cibernéticos no Brasil e no mundo estão crescendo e se diversificando muito rápido. A série de ataques mundiais ocorridos em 2017 emite um alerta sobre os enormes impactos que uma invasão digital pode causar, além do grau de vulnerabilidade que as empresas, públicas ou privadas, apresentam.

O Brasil está frequentemente presente entre os países mais visados pelos criminosos nos grandes estudos de golpes cibernéticos. Devido ao crescimento vertiginoso da internet por aqui, os ataques crescem em níveis muito mais elevados que em outros países. "Isso é alavancado por características singulares de um povo que deixa faltar a comida, mas tem seu smartphone sempre em dia, e pelo fato de o país ainda ser muito desorganizado em termos empresariais", afirma, categoricamente, o diretor comercial da NetSol, especializada em segurança de redes e internet, **Erasmo Borja Sobrinho**.

Durante muito tempo, o principal "motivador" dos hackers era apenas o dinheiro, ou seja, dados como os bancários e meios de pagamento. "Mas isso tem mudado um pouco. Hoje em dia, temos visto motivações políticas, religiosas e pessoais. Ou seja, todos os setores e tipos de informação são alvo potencial de um crime cibernético", afirma o gerente de linhas financeiras da seguradora AIG Brasil, **Flávio Sá**.

Cada segmento, diz ele, está exposto de maneira diferente, de acordo com os dados que possui e com as partes com as quais se relaciona. Considerando que o investimento em segurança da informação é finito, é necessário utilizar o conceito de "joias da coroa", ou seja, proteger os dados que são realmente valiosos para a organização.

As preferidas dos hackers são as empresas desprotegidas. "Atualmente, o que tem posto maior medo em todos nós são os chamados ransomwares", afirma Erasmo. É quando o hacker sequestra os dados e só os devolve mediante o pagamento de um valor, geralmente em bitcoin, a moeda virtual mais conhecida da internet.

A partir de um ciberataque, as empresas ficam expostas a perdas financeiras significativas e que trazem consequências à sua reputação e de seus usuários/clientes,

Divulgação

Divulgação

comprometendo o futuro da organização. “Além dos riscos reputacionais, há também os regulatórios, financeiros, operacionais e de propriedade intelectual”, ressalta Flávio.

## Sistemas de prevenção

Para se precaver das fraudes, o sistema de backup é um bom início, na avaliação do diretor da NetSol. “Mas o malware também pode contaminar o backup. Portanto, ele deve ser bem montado para evitar esses danos”, afirma. Um bom firewall é fundamental para a proteção da rede. “E precisa estar constantemente atualizado. A toda hora, novas formas de bloqueio são inventadas. As empresas de segurança têm que andar a par com os agentes do mal, com uma política estruturada para prevenir problemas”, observa Erasmo. O executivo alerta ainda que é necessário treinamento de usuários, normas de comportamento na rede corporativa, além de proteção extra contra uso de pendrives, por exemplo, já que podem conduzir vírus e contaminar o sistema de forma direta.

No caso de o ciberataque ter sido concretizado, Flávio recomenda que a melhor posição para a corporação é dar resposta rápida ao mercado. Segundo ele, é preciso que as empresas criem cultura de entendimento de riscos, desenvolvendo gestão específica para isso. Além das medidas tecnológicas para prevenir os ataques, diz, o seguro é um recurso importante para minimizar os riscos e o impacto de uma violação dos dados. Afinal, um ataque no sistema eletrônico da empresa pode significar a extinção ou a continuidade dos negócios. “Por isso, é de importância fundamental criar políticas de gerenciamento de riscos”, diz Flávio.

Banco de imagens - Freepik

# Segurança digital na lista de prioridades

A recomendação de que todas as "panes" e ataques nos computadores, e-mails e máquinas afins devem ser resolvidos somente pelos técnicos de informática das empresas mudou. É consenso global hoje o entendimento de que as organizações precisam corrigir a lacuna de comunicação entre as equipes de tecnologia e executivos para melhorar a proteção contra o furto de dados, além de investir mais na educação dos funcionários. Na prática, no entanto, isso não acontece. No Brasil, o roubo de propriedade intelectual e a violação envolvendo dados de clientes e perda de receita por parada do sistema muitas vezes são preocupantes apenas para a área de tecnologia da informação (TI).

A cibersegurança é assunto que deve estar na lista de prioridade de todos os escalões das empresas, pois os impactos das fragilidades nessa área são críticos para os negócios. Virou questão de sobrevivência. "A exposição dos dados pode causar desde a paralisação da empresa, por meio de sequestro de dados, até o pagamento de compensações judiciais por exposição de informações sensíveis de funcionários ou clientes, sem falar nas ações de espionagem industrial que podem levar a incalculáveis prejuízos", afirma o diretor-presidente da Concert Technologies, especializada em tecnologia da operação, **Ângelo Fares Menhem**. Seja qual for a situação, diz ele, o dano à imagem pública da empresa é muito grande.

E com a globalização, a empresa torna-se mais visível em escala mundial, atraindo, portanto, maior interes-

Divulgação

se em ataques. Ângelo ressalta que, como toda política empresarial, a cibersegurança precisa ser patrocinada pela alta gestão da companhia. "Como se trata de mudança cultural, todos os colaboradores devem ser envolvidos, com especial destaque para a gestão de pessoas e de TI", diz.

Banco de imagens - Freepik

*Mudança cultural depende do envolvimento de todos os colaboradores*

ENTREVISTA

# Cassio Jordão Motta Vecchiatti

Diretor do Departamento de Segurança (Deseg) e do Departamento de Competitividade e Tecnologia da Federação das Indústrias do Estado de São Paulo (Fiesp). É membro do Comitê Gestor da Internet no Brasil (CGI.br). Foi fundador e diretor-presidente da Associação Brasileira de Provedores de Acesso e Informação da Internet (Abranet).

Divulgação

**Quais os impactos dos ataques digitais na reputação das corporações?**

É cada vez maior. Embora os empresários ainda não estejam colocando a segurança dos dados como prioridade necessária, o impacto desses ataques interfere muito na reputação das empresas, que não cuidam desse ponto como deveriam.

**Com a internacionalização, há necessidade de as empresas focarem mais nos mecanismos de defesa cibernética? Por quê?**

Hoje vivemos em um mundo cada vez mais dependente da cibernética e da internet. Isso propicia a necessidade de atenção e implantação de mecanismos de defesa, pois a vulnerabilidade para ataques e roubo de dados só cresce.

**Quais as empresas sofrem mais riscos desses incidentes? As pequenas, médias ou grandes?**

Proporcionalmente, os riscos são semelhantes. Nas pequenas e médias, que normalmente têm menos proteção, a vulnerabilidade é maior, embora o interesse dos atacantes seja menor. Já as grandes empresas sempre têm mais proteção, mas o interesse pelos seus dados é maior, o que propicia ataques de pessoal mais habilitado. Dessa forma, eu poderia dizer que o risco é semelhante em todas.

**As empresas reconhecem que os ataques cibernéticos podem afetar de forma drástica os negócios? Ou essa preocupação ainda é incipiente no Brasil?**

Infelizmente, as empresas ainda não estão conscientes do risco que correm. Essa consciência só chega quando sofrem um ataque e têm seus dados subtraídos.

**Quais políticas devem ser adotadas pelas empresas para proteger suas informações digitais?**

Elas devem adotar políticas de treinamento específicas a cada caso e criar regras e manuais internos para proteção de seus dados. Eu me refiro tanto ao uso de equipamentos, como computadores e smartphones, a treinamento constante e permanente de seus funcionários de todos os escalões. O processo evolutivo do mundo virtual é tão dinâmico que algo inventado hoje, amanhã, estará velho e superado se não for adequado permanentemente.

**Quais os principais danos que as empresas podem sofrer com os ataques cibernéticos?**

A perda dos próprios dados, que pode paralisar a empresa. O roubo de informações de seus processos pode causar concorrência predatória.

**É importante que esse trabalho de proteção dos dados seja feito em parceira por gestores, equipe de TI e trabalhadores?**

Para adotar a política de proteção de dados, é preciso, primeiramente, que a administração da empresa esteja consciente e determinada a implantar esses processos, que hoje são fundamentais para a própria sobrevivência. Conscientes disso, a determinação de políticas deve envolver todos, desde o faxineiro até o presidente. Isso é fundamental para proteção dos dados da empresa.

**Qual o perfil desejado do profissional da segurança da informação?**

Além do conhecimento na área de segurança da informação, precisa saber da empresa e de seus processos produtivos. Pouco vale ter um PHD em segurança cibernética se a pessoa não conhece a empresa. Entendo que, em grande parte dos casos, o treinamento em TI de um bom funcionário que conheça a empresa é o caminho mais eficaz. Esse assunto não é mais só de TI e necessita ser reconhecido como tema crítico de negócios nas empresas. Portanto, o caminho é a conscientização dos gestores e treinamento, treinamento, treinamento...

# Banco é alvo preferencial para ciberataque

O setor bancário no Brasil continua sendo o mais visado e com maior risco de ciberataques. É o que aponta o relatório *Cenário dos crimes cibernéticos 2015-2016*, elaborado pela NS Prevention, unidade de prevenção a fraudes e análise de riscos do grupo New Space, empresa brasileira especializada em serviços de tecnologia para o setor financeiro. O segmento é constantemente alvo de criminosos que buscam os recursos financeiros, mas também o acesso às informações de clientes, ao banco de dados e às senhas, entre outras informações sigilosas.

A gerente de Estudos Regulatórios da Associação Brasileira das Entidades dos Mercados Financeiro e de Capitais (Anbima), Patrícia Menandro, enfatiza que ataques cibernéticos representam riscos muitos graves para instituições dos mercados financeiro e de capitais. "Não somente riscos relacionados diretamente à integridade das operações que realizam para seus clientes, mas riscos de contágio, de imagem, de quebra de confiança, todos assuntos fundamentais para a continuidade de suas atividades".

Além dos prejuízos causados pelo furto de contas, tem crescido o percentual de problemas causados pelas chamadas ameaças internas involuntárias, geralmente resultado da falta de informação de segurança ou negligência das organizações. Estão incluídos aí os descuidos por parte dos colaboradores – como abrir e-mails de destinatários desconhecidos ou links e arquivos anexos que pareçam suspeitos – e os ataques propositais de dentro da própria empresa, como vazamentos de dados.

Para evitar prejuízos, as instituições financeiras têm ampliado cada vez mais seus investimentos em segurança, com sistemas de criptografia de dispositivos tecnológicos, testes de phishing, melhoria de controle de spam, dupla autenticação de senhas para acesso a redes, atualização de aplicativos e firmware e na implantação de boas práticas de gerenciamento de dados sigilosos.

Buscando contribuir para o aprimoramento das práticas de segurança cibernética, a Anbima publicou, em agosto de 2016, o Guia de Cibersegurança, que recomenda algumas práticas para implantação de um programa de segurança cibernética das instituições. Dentre elas, avaliação de riscos, governança, controle e conscientização dos usuários, controles tecnológicos e físicos, plano de resposta a incidentes, processos de investigação, diálogo com partes externas, prevenção de ataques internos e acesso à informação.

O documento sugere ainda a adoção de medidas básicas de cibersegurança, como definição de papéis e responsabilidades e de perfis de acesso aos sistemas, à rede e à base de dados e servidores; regras para definição de senha; monitoramento do uso de internet; regras para download e para upload; controles para utilização de e-mails, mídias e periféricos; trilhas de auditoria e guarda dos logs; regras de backup; controle de entrada e saída de equipamentos e de prestadores de serviço; utilização de softwares de segurança; classificação da informação; ciclo de vida da informação e disseminação da cultura de segurança.

**SEGURANÇA DA INFORMAÇÃO EM INSTITUIÇÕES FINANCEIRAS**

- **65% dos executivos do setor financeiro no Brasil disseram que suas instituições estudam implementar blockchain.**
- **29% já avaliam experiências analytics e computação cognitiva ou inteligência artificial.**

*Fonte: Pesquisa Febraban de Tecnologia Bancária 2017*

**PRINCIPAIS CIBERATAQUES SOFRIDOS PELAS ORGANIZAÇÕES FINANCEIRAS**

**81% das violações exploraram senhas roubadas e/ou fracas.**
**43% dos incidentes foram ataques sociais.**
**51% das violações incluíam malware.**
**66% dos malwares foram instalados via anexos maliciosos de e-mail.**
**73% das violações eram financeiramente motivadas.**
**21% das violações estavam relacionadas à espionagem.**
**27% das violações foram descobertas por terceiros.**

*Fonte: Relatório Verizon*

Anbima

Patrícia destaca que o Guia de Cibersegurança foi construído para ser um referencial para a divulgação da cultura da cibersegurança. "A Anbima considera importante auxiliar na identificação das práticas e procedimentos mínimos que devem ser adotados para mitigar riscos cibernéticos e orientar a implantação de uma política de cibersegurança que mapeie riscos, contribua para a resiliência e a capacidade de responder a ataques e eduque as equipes nessa direção". O guia é aplicável a instituições de diversos portes e que atuam em diferentes segmentos do mercado de capitais.

A Anbima avalia que houve uma ampliação da cibersegurança no setor desde a primeira edição do guia. "Nosso balanço é muito positivo e, com certeza, é um assunto que veio para ficar na agenda estratégica das instituições. Estamos aprimorando o documento e acrescentando novas orientações", ressalta Patrícia.

# Blockchain e a segurança do sistema financeiro

Uma tecnologia da informação tem chamado a atenção das instituições financeiras pelo potencial em reduzir custos operacionais, pelo ganho de eficiência e aumento da segurança. O sistema blockchain, ou DLT (sigla em inglês para livro-razão distribuído), permite criar registros encadeados e dependentes entre si, sem controle centralizado, possibilitando que transações financeiras sejam distribuídas e verificadas por diversos pontos da rede, com garantia de autenticidade.

Iniciativas para a implantação de blockchain nas instituições financeiras no Brasil já estão sendo feitas. A Federação Brasileira de Bancos (Febraban) criou, em agosto de 2016, um grupo de trabalho (GT) para desenvolver estudos sobre a aplicação dessa tecnologia. Participam Banco do Brasil, Bancoob, Banrisul, Bradesco, BTG Pactual, Caixa, Citibank, Itaú Unibanco, JP Morgan, Safra e Santander, além do Banco Central, Câmara Interbancária de Pagamentos (CIP) e B3, empresa decorrente da fusão da BM&FBovespa e a Cetip.

O grupo de trabalho já desenvolveu duas provas de conceito de blockchain para testar diferentes plataformas com base em um cadastro digital fictício de cliente, com capacidade de compartilhamento entre diferentes instituições e atualização em tempo real.

A primeira prova, chamada Fingerprint, foi desenvolvida na Corda (plataforma blockchain criada por um grupo com mais de 70 das maiores instituições financeiras do mundo, em um consórcio montado pela R3, empresa de tecnologia financeira sediada em Nova Iorque), que usa o conceito de DLT. Esse protótipo envolveu Itaú, Bradesco e B3 e foi apresentado no 1º Seminário Blockchain Febraban, realizado em abril de 2017. A iniciativa comprovou a capacidade dos bancos de operarem de forma colaborativa.

A segunda foi apresentada em junho deste ano no Congresso e Exposição de Tecnologia da Informação das Instituições Financeiras. O protótipo chamado DNA foi desenvolvido em Hyperledger (projeto colaborativo envolvendo várias indústrias, iniciado em dezembro de 2015 pela Linux Foundation, para suportar livros-razão distribuídos com base no blockchain). A prova de conceito apresentou um produto fictício no ambiente virtual do setor bancário e teve a participação de todas as instituições do GT Blockchain da Febraban. A partir desses testes, foi possível avaliar a capacidade das plataformas, as diferenças entre elas e os aspectos relacionados ao desenvolvimento do sistema. A próxima etapa será a realização de um projeto-piloto de blockchain que está em fase de criação.

Arquivo pessoal

## Desafios

O representante do Blockchain Research Institute no Brasil, **Carl Amorim**, acredita que o principal desafio para implantação de tecnologias de blockchain no país é cultural. "A tecnologia de blockchain já existe, e qualquer organização ou governo pode implantá-la. Porém, vivemos em uma sociedade baseada em sistemas centralizados e isso acontece também com os modelos de negócios das empresas. Para conseguirmos usar melhor essa tecnologia, isso precisa mudar. Outros sistemas organizacionais mais apropriados ainda são recentes. É preciso quebrar nossas próprias resistências para usarmos essa tecnologia com eficiência e eficácia", acredita Amorim, que é também editor e tradutor do livro *Blockchain Revolution*, de Don Tapscott.

Ele aponta ainda como desafio a quantidade de operações realizadas pelas instituições financeiras. "Os bancos processam milhões de transações por segundo. O blockchain não chegou a esse número. Não dá pra comparar essa escala".

**Fernando Bresslau**, professor de pós-graduação em empreendedorismo e blockchain na Faculdade de Informática e Administração Paulista (Fiap) e Escola Superior de Propaganda e Marketing (ESPM) e Country Manager Brazil da Ripio – startup pioneira em criptomoedas na América Latina, também enumera alguns obstáculos. "Blockchains são sistemas muito complexos que utilizam processos de incentivo para funcionar. Desenvolver bons sistemas de incentivo é certamente uma barreira. Além disso, não faz muito sentido elaborar sistemas internos, utilizados apenas por uma empresa, pois blockchains foram criados para serem usados em rede. Encontrar um consenso com os membros dessa rede sobre a utilização do sistema é muito difícil".

Bresslau ressalta ainda a dificuldade das organizações em lidar com uma tecnologia tão recente. "Há muito o que aprender, e não existem muitas boas práticas difundidas, nem profissionais capacitados no mercado. Todos esses aspectos tornam o desenvolvimento de sistemas blockchain arriscado, caro e, possivelmente, demorado", considera. No entanto, ele defende que o blockchain possa contribuir para a cibersegurança das instituições financeiras. "A tecnologia dele é baseada em conceitos que, em conjunto, fazem com que o sistema seja muito seguro. Funções de hash, referenciamento consecutivo de transações e assinaturas criptográficas digitais são ferramentas que podem ser utilizadas para torná-lo mais seguros".

Amorim comenta que é praticamente impossível fraudar um sistema de blockchain. "Para fazer isso, seria necessário hackear todos os nós, todos os computadores da rede que fazem o processamento. No caso do blockchain do bitcoin (uma criptomoeda), são cerca de dez mil máquinas que fazem a verificação e a validação das transações. Não há tecnologia no mundo capaz de fazer isso", afirma.

A utilização de criptomoedas, na opinião de Bresslau, faz com que o usuário tenha maior preocupação com a própria segurança digital, o que também contribui para a cibersegurança. "Se esse usuário for cliente de um banco, começará a ter mais cuidados também com o acesso ao internet banking e o uso do aplicativo, o que é positivo para o setor".

Os dois especialistas afirmam que um sistema blockchain bem desenvolvido pode trazer vantagens ao consumidor final das instituições financeiras. Para Bresslau, o cliente terá a certeza de que as regras acordadas não possam ser manipuladas pelos prestadores de serviço; da maior transparência em relação às transações junto à instituição; da simplificação

Arthur Fujii

nos processos burocráticos, com a eliminação de agentes e passos intermediários. "Isso deve se traduzir em maior agilidade e menores custos para o banco e para o consumidor".

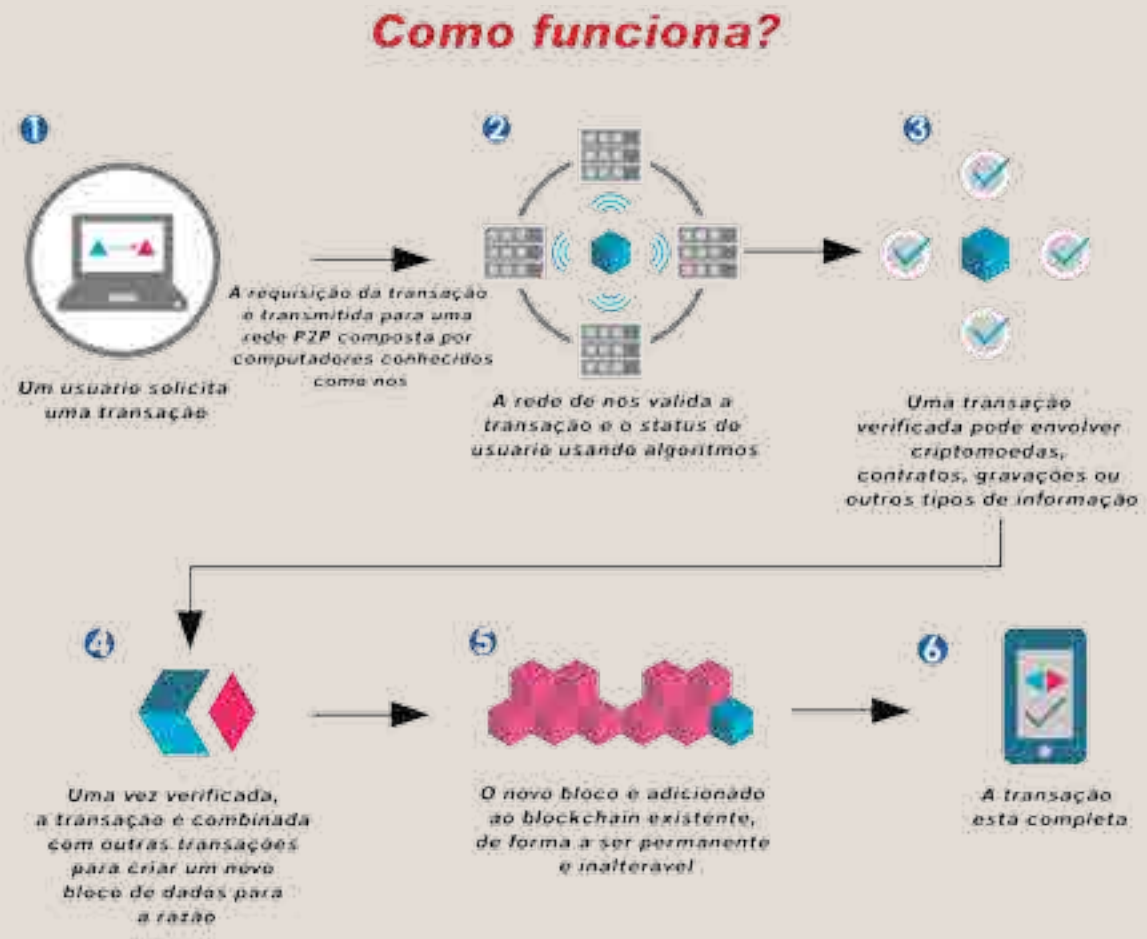
Para Amorim, o principal benefício será a criação de novos mercados. "A partir da utilização de blockchain, as instituições financeiras poderão realizar operações mais precisas com custos infinitamente menores, tornando-se mais ágeis e mais transparentes. Isso pode representar a inclusão de uma massa de usuários que antes não tinha acesso ao serviço".

Ainda sobre a inclusão de novos clientes, Amorim acredita ser necessária uma mudança na cultura empresarial dos bancos. "Eles precisam parar de olhar para o mercado e achar que já tem um tamanho tal que não vai mais mudar. Ou as instituições financeiras incluem essas pessoas ou elas vão procurar soluções para suas demandas entre elas, longe do sistema bancário".

Douglas Gonçalves, chief technology officer e sócio da Carambola Tech, empresa de soluções tecnológicas e desenvolvimento de ambientes digitais de alta performance, que atua em projetos que envolvem Agile, internet das coisas, inteligência artificial e blockchain, o maior desafio no Brasil e no mundo é a formação das pessoas. "Precisamos tanto de técnicos como de engenheiros de software, desenvolvedores, especialistas em infraestrutura, como advogados, investidores, pessoal de negócios, etc. Só quando tivermos pessoas suficientes que conheçam bem o assunto é que teremos o uso massivo das possibilidades que o blockchain nos permite".

### *BLOCKCHAIN*

**Sistema de arquivos distribuído em diversos computadores, no qual transações de troca de valores são agrupadas em blocos de maneira sequencial. O arquivo é composto de blocos, no qual cada um inclui uma assinatura criptográfica do bloco anterior, criando um registro imutável. Não há intermediários, tudo funciona de forma descentralizada. A tecnologia é protegida por avançados e complexos sistemas de criptografia. Como um grande e confiável livro de contabilidade, é um ambiente ideal para reguladores e auditores.**



# Bitcoin: moeda digital preferida por compradores virtuais

Uma iniciativa capaz de agradar ao mesmo tempo investidores que buscam formas inovadoras para ganhar dinheiro e idealistas que questionam o poder das megacorporações financeiras. O bitcoin conquistou esses grupos tão distintos e tornou-se a criptomoeda mais bem-sucedida e preferida entre aqueles que compram regularmente pela internet ou fazem transações financeiras internacionais.

O pesquisador do Instituto de Tecnologia e Sociedade (ITS) Rio, **Gabriel Aleixo**, cofundador da STAR Labs (Laboratórios de Pesquisa Avançada Científica e Tecnológica), acredita que um dos motivos do sucesso do bitcoin é o fato de ele ser uma forma mais rápida e mais barata que os meios tradicionais de pagamento para inúmeros casos. "Para remessas internacionais de valores a parentes e afins, para contratação de freelancers internacionais, para compra de bens digitais (jogos ou serviços de infraestrutura tecnológica, como hosting) ou até mesmo viagens, há uma grande eficiência ao usar moedas digitais".

Thiago Dias / ITS Rio

Essa criptomoeda tem sido cada vez mais utilizada por quem gosta de fazer compras pela internet. "Ela se mostra uma forma perfeita para quitações, já que é prático para quem compra e irreversível para quem vende. Isso é algo inédito em um meio digital de pagamento, dado que, quando se utilizam cartões ou intermediários tradicionais, há possibilidade de estorno, o que algumas vezes é um recurso utilizado para fraudes", destaca Aleixo.

Remunerar utilizando a moeda digital pode trazer, ainda, economia para o usuário. Nos Estados Unidos, a fabricante de computadores Dell já a aceita em seu e-commerce e oferece descontos de até 10%. O bitcoin está em circulação há quase uma década no mundo todo e já é aceito em mais de 15 mil estabelecimentos no Brasil, entre lojas físicas e virtuais, bares, hotéis, entre outros prestadores de serviço. Apesar disso, a assimilação dele pelo público em geral ainda é considerada a maior desvantagem, de acordo com Aleixo. "Embora se trate de algo mais simples de usar que muitos imaginam, sem dúvidas, há certa curva de aprendizado que deve ser transposta para se pagar por algo com bitcoins pela primeira vez", ressalta.

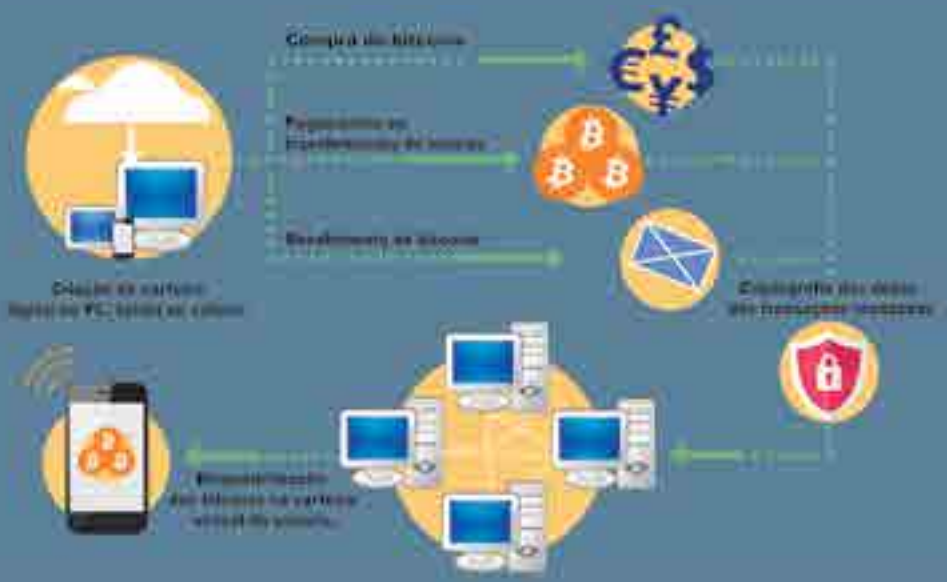
Outra barreira para a popularização dele é o considerável risco do investimento, devido à alta volatilidade da moeda virtual, uma vez que o preço é determinado puramente pela ação contínua de compradores e vendedores no mundo todo, sem qualquer interferência externa. "Quando há valorização, pode ser interessante para quem vê na moeda um veículo de investimento ou poupança em longo prazo. Entretanto, em caso de desvalorização, poderá ser necessário dispender um valor maior que o esperado para realizar a aquisição de bem ou o pagamento pelo provimento de um serviço", observa o pesquisador.

## *COMO FUNCIONA*

A principal característica do bitcoin é que a própria rede valida as transações. Não é necessária uma autoridade financeira, como o Banco Central, para regulamentar o funcionamento desse tipo de moeda. Para adquiri-la, inicialmente, é preciso criar uma carteira virtual no site oficial da blockchain (https://www.blockchain.com/). Essa carteira funciona como uma espécie de conta bancária, livre de taxas e impostos, em que ficam armazenados todos os bitcoins. A carteira virtual possui uma numeração específica, protegida por criptografia, e armazena cada transação com todas as informações – data, de quem para quem, quais os valores trocados.

Por ser uma moeda virtual, não pode ser impresso, e precisa ser "minerado". A atividade "mineração" tem sido realizada no mundo todo e tornou-se, inclusive, fonte de renda para quem tem condições de investir em computadores de alta performance. As potentes máquinas são necessárias para resolver os algoritmos matemáticos gerados para validar cada pagamento realizado com bitcoins. A cada dez minutos, as transações pendentes na rede são verificadas pelos mineradores e agregadas em um bloco, que é transformado em um algoritmo. Ao resolver esse algoritmo, os mineradores recebem um valor em bitcoins pelo serviço e uma taxa para cada transação.

Além de incentivar a atuação dos mineradores, a atividade também possibilita novas emissões da moeda. Contudo, por convenção, a mineração de bitcoins está limitada a 21 milhões de moedas digitais, sendo que mais de 16 milhões delas já estão em circulação.



# Quanto vale

O valor é determinado pela demanda. Quanto maior a quantidade de transações financeiras, maior a cotação da criptomoeda. Desde a sua criação, em 2008, a moeda virtual tem apresentado alta volatilidade. Em 2014, o bitcoin sofreu forte desvalorização, devido à comercialização de ativos no mercado futuro e ao ataque de hackers em empresas negociadoras especializadas em transações virtuais. Atualmente, a criptomoeda tem apresentado forte valorização, em especial nos primeiros cinco meses de 2017. Em 1° de janeiro, o bitcoin era negociado a pouco mais de mil dólares. Já no final de maio, valia mais de 2,4 mil dólares.

Para Gabriel Aleixo, a perspectiva futura do mercado de criptomoedas é de crescimento. "Em especial para compra e venda de bens puramente digitais, bem como para contratação de serviços internacionalmente ou remessas de valor entre partes distantes, creio que a tendência de uso das moedas digitais é a de grande crescimento no Brasil e no mundo".

O pesquisador aponta também que o aumento do ceticismo frente aos meios financeiros tradicionais e a possibilidade de novas crises podem levar ao crescimento dessa moeda digital como meio de reserva de valor. "Mais pessoas começarão a investir uma parte, mesmo que pequena, de suas poupanças e investimentos em bitcoins, como forma de preservar valor em algo independente do sistema tradicional ao longo do tempo, uma vez que ele é imune a políticas monetárias ruins, por exemplo".

## CRESCIMENTO DA VALORIZAÇÃO


*Fonte:https: //blockchain.info/pt/charts/market-price*

# O misterioso criador do bitcoin

O bitcoin surgiu em 2008, após a publicação do artigo *Bitcoin: a peer-to-peer electronic cash system* (Bitcoin: um sistema de dinheiro eletrônico ponto a ponto), assinado pelo pseudônimo Satoshi Nakamoto. Até hoje, não se sabe a real identidade do criador ou o grupo de pessoas que criou a moeda digital.

Nakamoto propôs um sistema descentralizado para realizar transações eletrônicas sem necessidade de instituições financeiras para concretizá-las. O sistema se baseia em assinaturas digitais para garantir a confiança das operações e evitar falsificações como o duplo uso da moeda digital.

Conforme descreve o artigo, a rede faz um registro temporal com todas as informações de cada transação, que é, em seguida, verificada e processada em blocos encadeados de assinaturas digitais por vários nós dentro de uma rede peer to peer (arquitetura de redes de computadores em que cada um dos pontos ou nós da rede funciona tanto como cliente quanto como servidor, o que permite compartilhamentos de serviços e dados sem a necessidade de um servidor central). Quanto maior a cadeia de blocos, maior a confiança das transações.

O mais representativo uso em larga escala do bitcoin já registrado foi em transações realizadas no Silk Road, um site de venda ilegal de drogas que operava na deep web e que foi tirado do ar pelo FBI em 2013. Estima-se que tenham sido movimentados, na cotação atual, quase 3,6 milhões de dólares em bitcoins. O valor foi apreendido pelo FBI naquela que foi considerada a segunda maior apreensão de dinheiro já realizada pela instituição em toda a sua história.

Blockchain é a estrutura de dados que representa uma entrada de contabilidade financeira ou um registro de uma transação. Cada transação é digitalmente assinada para garantir sua autenticidade e integridade.

## PAÍSES QUE CONSIDERAM ILEGAL A UTILIZAÇÃO DE BITCOINS

Afeganistão | Bangladesh | Equador | China* | Bolívia | República da Macedônia

* Utilização restrita somente para transações virtuais, com possibilidade de futura proibição

*Fonte: Site Coin Dance – Serviços e estatísticas sobre bitcoins*

# Internet das coisas já é realidade

O termo internet das coisas (em inglês, Internet of Things – IoT) já deve ser encarado como realidade mundial e algo inevitável. É o apelido dado à revolução tecnológica que tem como objetivo conectar os itens usados no dia a dia à rede mundial de computadores. Cada vez mais surgem eletrodomésticos, meios de transporte e até mesmo tênis, roupas e maçanetas conectados à internet e a outros dispositivos, como computadores e smartphones. Por meio da internet das coisas, os objetos ganham vida nas redes.

A ideia é que, cada vez mais, o mundo físico e o digital se tornem um só, por meio de dispositivos que se comuniquem com os outros, os data centers e suas nuvens. A estimativa de vários institutos de pesquisa é que mais de 30 bilhões de dispositivos irão formar uma internet das coisas em 2020. Os defensores da inovação dizem que os benefícios para os consumidores são substanciais, como melhoria do bem-estar e até mesmo economia de tempo e dinheiro em longo prazo, com a redução do desperdício de recursos naturais e energéticos, por exemplo.

Os objetos conectados à internet e outros dispositivos fizeram surgir principalmente sensores que podem sentir o ambiente e ter métricas, tais como temperatura, umidade, pressão, vibração e composição de nutrientes do solo numa determinada área, vaga ocupada ou livre em estacionamento. "A IoT poderá melhorar a utilização de recursos energéticos e promover sustentabilidade", afirma a professora do Instituto Federal de Educação, Ciência e Tecnologia de Goiás (IFG), *campus* Lusiânia, **Christiane Borges Santos**.

Alguns sensores podem armazenar em suas memórias um histórico das últimas métricas e interagir conforme programas e acessos às redes. "E podem acionar atuadores para mudar *status* das coisas, ligando um motor, programando ajuste de temperatura, invalidando a utilização de um remédio que teve sua temperatura acima do limite determinado e assim por diante", afirma o engenheiro eletrônico João Neves, diretor do Fórum Brasileiro de Internet das Coisas, criado com o objetivo de alertar para a importância da IoT e identificar os obstáculos que dificultam a adoção do conceito no Brasil.

Com a revolução, podem ser criadas soluções de problemas e oferta de serviços antes inimagináveis. "O céu é o limite.

Divulgação

Os recursos da tecnologia estão aí à mão para quem tiver imaginação e arrojo", afirma João Neves, que tem mais de 40 anos de experiência na área de informática. "Gadgets que gravam informações pessoais, como biometria, saúde e localização também estão na categoria de 'coisas' em IoT", explica a professora Christiane. Ela afirma que a internet das coisas promove economia com novos modelos de negócios, que melhoram a experiência e criam novas formas de se relacionar com clientes, traz novos produtos e serviços, assim como inova na análise e aplicação de inteligência sobre dados exclusivos coletados.

O fórum, formado por representantes do mercado, da academia e do governo, é o organizador do Congresso Brasileiro e Latino-Americano de Internet das Coisas, que teve sua segunda edição em setembro deste ano em São Paulo e reuniu mais de 300 pessoas, entre expositores e renomados debatedores nacionais e internacionais. É ainda o grande inspirador para a realização do Plano Nacional de Internet das Coisas, uma realização pública com o apoio do Banco Nacional de Desenvolvimento Econômico e Social (BNDES) e diversos empresários e entidades, ouvidos pelo Ministério da Ciência, Tecnologia, Inovações e Comunicações (MCTIC). O plano tinha prazo para ser concluído em outubro deste ano e

definiria os rumos para ações em todos os âmbitos, com diretrizes para impulsionar a criação de novas tecnologias. É ambicioso e tenta colocar o Brasil em posição de liderança no segmento.

## O lado ruim da IoT

Apesar da série de benefícios da IoT, é preciso mencionar preocupações críticas sobre privacidade e segurança. Se, por um lado, vem para facilitar e tornar mais prática a vida das pessoas, o fato de tudo estar interligado sem o uso de fios exige medidas de segurança impecáveis, especialmente se o dispositivo em questão é o que se refere à vida humana. Dentre os riscos, contam-se não apenas o roubo de dados, como também ferimentos físicos ou até mesmo mortes.

A coisa fica assustadora quando se fala de softwares de saúde. Muitos marcapassos modernos se comunicam com computadores para produzir dados médicos sobre o quadro cardiovascular do paciente. Mas a conexão envolve riscos, pois falhas em softwares de funcionamento podem permitir a intervenção de hackers. Ou seja, é possível invadir e desativar esses dispositivos implantados no corpo de quem possui problemas cardíacos.

Na Universidade do Alabama, nos Estados Unidos, que tem um dos simuladores do corpo humano mais realistas do mundo, um grupo de alunos conseguiu invadir a conexão, acelerar e reduzir a frequência cardíaca do falso humano e provocar a morte do robô. Isso com pouca experiência específica sobre ataques a sistemas. E eles garantiram que o mesmo pode ser feito em marcapassos e bombas de insulina de humanos de verdade.

Sentados sossegadamente num sofá, um grupo de hackers pode ligar o laptop, conectar-se à internet e invadir um veículo que trafega em estradas. Várias marcas que são sinônimos de carro elétrico já sofreram com esses testes, muitos realizados por hackers whitehats (chapéus brancos), considerados do bem. Em geral, são estudantes, engenheiros de computação e especialistas em tecnologias digitais que costumam ser contratados por empresas para descobrir brechas. Eles costumam invadir sistemas eletrônicos alheios e avisam companhias sobre as vulnerabilidades que descobrem.

Com a vida inteira conectada, à medida que mais aparelhos com acesso à internet entram em casa para facilitar o dia a dia, mais pessoas ficam vulneráveis aos ataques cibernéticos, inclusive à invasão de privacidade. "Os mais preocupantes problemas de segurança são relacionados a questões de privacidade, falta de criptografia segura, configurações padrão e falta de senhas complexas", afirma Christiane. Muitos dispositivos, diz ela, enviam dados de consumo e informações pessoais do usuário, como endereço de e-mail, data de nascimento, estado de saúde e números dos cartões de crédito para os fabricantes.

Segundo João Neves, a preocupação das empresas em redefinir os sistemas de segurança e criar novas plataformas de serviços e modelos de TI deve ser permanente, pois uma coisa interagindo com outra, fazendo medição ou acionamento, não deve ser facilmente invadida e ter seus valores e processos alterados.

"A segurança é um dos requisitos mais importantes, mas nem sempre é o foco das empresas que desenvolvem hardware para implementação de soluções de IoT", afirma a professora Christiane. Com a segurança como item secundário, operações e dados críticos da rede e de usuários estão em risco. Diante desse cenário, tornam-se necessários investimentos em componentes de arquitetura mais inteligentes, incluindo a proteção dos dados em qualquer lugar e soluções de criptografia e uso de senhas complexas.

# O QUE É INTERNET DAS COISAS?

Empresas e organizações explicam a internet das coisas de várias maneiras. Trata-se, em geral, de uma rede de objetos físicos, prédios, veículos e outros dispositivos que possuem tecnologia embarcada, sensores e conexão de rede, capazes de coletar e transmitir dados através de redes para softwares e aplicações. É a conexão global de "objetos inteligentes" por meio da estrutura da internet. Com ela, é possível a comunicação direta entre diversos dispositivos de uso pessoal, bem como entre estes e seus usuários, utilizando sensores e conexões sem fio.

Um objeto "inteligente" possui nome e endereço na internet, tem a capacidade de se comunicar enviando e recebendo informações com outros dispositivos, interage com essas informações recebidas e possui algum sensor de fenômenos físicos (velocidade, luz, calor, eletromagnetismo, radiação, etc.). O termo internet das coisas já até entrou para a lista sagrada do dicionário inglês Oxford, de palavras relacionadas à linguagem da internet e tecnologia, como emojis (figurinhas de expressões para mensagens) e selfies (autorretrato).

## APLICAÇÕES DA INTERNET DAS COISAS

- **CIDADES INTELIGENTES:** ambientes urbanos conectados.
- **TRANSPORTE:** o carro do futuro compartilhará dados com a nuvem, com a infraestrutura e com outros veículos. Existem ainda aplicações para transporte coletivo, monitoramento e manutenção de rotas, controle de tráfego e pedágio eletrônico.
- **INSTALAÇÕES PREDIAIS:** escritórios, fábricas, lojas de varejo e outras instalações comerciais de hoje em dia estão se transformando em edifícios inteligentes.
- **REDE ELÉTRICA:** inúmeros dispositivos da rede de energia elétrica podem compartilhar informações em tempo real para distribuir e gerenciar a energia, garantindo eficiência operacional e medição inteligente.
- **INDUSTRIAL:** permite que as fábricas aumentem a colaboração entre máquinas, seres humanos e sistemas empresariais – desde a cadeia de suprimentos até o chão de fábrica. É possível o monitoramento e a manutenção remotos de equipamentos industriais.
- **WEARABLES (TECNOLOGIAS VESTÍVEIS):** diferentes acessórios podem ser fonte de informação, comunicação, entretenimento ou assistência médica para os seus utilizadores.

# OBJETOS ELETRÔNICOS A CAMINHO

- Lâmpadas inteligentes ganham aplicativo com controle para escolher cores e para ligar e desligar.
- Lista de compras da geladeira pode ser preenchida automaticamente quando um determinado produto se aproxima da data de validade ou do consumo completo.
- Medicamentos podem enviar lembretes para o paciente informando prescrição, data de validade e horário de ingestão.
- Tênis com bluetooth vibra para ajudar a achar o caminho.
- Sistemas inteligentes e on-line poderão monitorar os elevadores por meio de call centers e técnicos. O intuito do programa é prestar assistência em tempo real e evitar acidentes com manutenções preventivas, além da redução de custo.
- O marcapasso envia informações em tempo real ao médico responsável pela garantia de sua saúde.
- O smartphone corporativo controla dados e serve como meio de pagamento de contas pessoais e empresariais.
- O interior dos automóveis também pode ser reiventado. Ao entrar em um carro com essa tecnologia, uma câmera vai fazer o reconhecimento do rosto do motorista, a fim de oferecer informações sobre seu cotidiano, recomendar músicas e receber orientações para acionar o mapa com GPS. Se o sistema não reconhecer a pessoa, ele tira uma foto e manda as informações para o celular do dono, evitando furtos.

# De olhos bem abertos

Os sistemas eletrônicos estão cada vez mais aprimorados para identificar as ações e as informações dos usuários. E com esses dados pessoais em mãos, as empresas podem usá-los para facilitar a rotina de muitas pessoas, com dicas personalizadas de produtos e serviços. Mas eles também podem ser usados para o mal, com ataques a seguranças física e financeira. A cautela deve começar na hora de abrir o e-mail ou sites que não são familiares, além de downloads de documentos, fotos, músicas ou vídeos sem saber a procedência.

Grande parte das artimanhas eletrônicas começa com o phishing. As páginas clonadas de bancos ou varejo on-line, segundo os especialistas, figuram entre os grandes golpes, pois atingem volume expressivo de pessoas. "Se os hackers mandarem 1 milhão de e-mails com mensagens de instituições financeiras e 1% dos internautas cair no golpe, já são 10 mil pessoas que podem ter informações violadas", afirma o professor de criptografia e segurança do Departamento de Ciência da Computação da Universidade Federal de Minas Gerais (UFMG), o holandês Jeroen van de Graaff.

Para o leigo, diz ele, é difícil detectar se esse contato é oficial da instituição financeira ou empresa que procura. "É preciso saber, no entanto, que informações bancárias, como senhas, não são solicitadas por e-mail", afirma Jeroen. Os dados do cartão de crédito são os que requerem maior cuidado, segundo o professor. "Os outros, como CPF e Carteira de Identidade, hoje em dia são quase públicos", diz.

Divulgação

O usuário é afetado principalmente quando a empresa onde está cadastrado é atacada, observa o fundador da Perallis It Inovation, **Vinícius Perallis**. Ela atua com segurança de dados, programas de conscientização de cibersegurança, avaliação e planejamento de defesa cibernética. "Muitas empresas não informam aos usuários que seus dados foram violados, mas são obrigadas a fazer isso e prestar a assistência necessária", afirma Vinícius.

A velha máxima de que anotar as senhas em papelzinho é um erro é desmistificada pelo professor Jeroen. "Muitas vezes pode ser mais seguro que ter um arquivo com essas informações no computador ou no celular. Mas se o equipamento é violado, todos os dados ficarão nas mãos do hacker", afirma. Segundo o professor, há vários programas para procurar senhas em dispositivos digitais. "Mas para achar em papel, obviamente que não há", diz. A combinação, na sua avaliação, não precisa ser tão complexa, mas inesperada. "Já usei os números da placa do carro ao contrário", diz.

### *O QUE É PHISHING*

É uma técnica de fraude on-line, utilizada por criminosos do mundo digital para roubar senhas e outras informações pessoais, usando-as de maneira fraudulenta. A expressão phishing (pronuncia-se "fichin") surgiu a partir da palavra em inglês "fishing", que significa "pescando". Ou seja, os criminosos utilizam essa técnica para "pescar" os dados das vítimas que "mordem o anzol" lançado pelo phisher ("pescador"), nome que é dado a quem executa um phishing. A tentativa de phishing pode acontecer por meio de websites ou e-mails falsos, que imitam a imagem de empresa conhecida e confiável para poder chamar a atenção das vítimas. Normalmente, os conteúdos dos sites ou e-mails com phishing prometem promoções extravagantes ou solicitam a atualização dos seus dados bancários.

*Fonte: Gallo Tecnologia da Informação*

Banco de imagens - Freepik

*Especialistas alertam os pais sobre os perígos que a internet pode oferecer às crianças e aos jovens*

Ele recomenda a modificação das senhas a cada ano. "Acho que uma vez a cada dois meses é exagero". "Essa questão do período é polêmica. O mais importante é que sejam seguras", completa Vinícius. E as senhas mais importantes, na avaliação de Jeroen, devem ser variadas. "Se o violador encontra, vai acessar todas as informações, pois eles sabem que as pessoas costumam usar sempre a mesma. E os hackers têm programas que testam isso", afirma.

O antivírus eficiente nas máquinas pode ajudar no processo de proteção, assim como os softwares para armazenar senhas, que geralmente usam a criptografia. Os usuários devem ficar atentos às atualizações dos softwares para minimizar as vulnerabilidades e evitar a instalação desse tipo de vírus. Por isso, é preciso sempre baixar a versão mais recente assim que ela estiver disponível.

Para não ser alvo de hackers, Vinícius recomenda distância de sites de pornografia, consumo ilegal e fofocas. "São apelativos e perigosos. E o objetivo muitas vezes é explorar as fraquezas do ser humano", observa. Tanto os dados do celular como do notebook devem ser criptografados, segundo ele.

Outra sugestão do empresário, que é estrategista em cibersegurança, é verificar se seu e-mail está em alguma lista de vazamento de dados circulando na

### *PROTEJA-SE*

- **Tenha senha extensa e não a anote em lugar visível.**
- **Altere senhas (não use a mesma para várias transações, pois se é descoberta, informações em diversos sistemas podem ser violadas).**
- **Habilite duas senhas toda vez que houver essa opção na máquina.**
- **Nunca deixe o site de compras gravar os dados do cartão de crédito (alguns bancos já geram um número só para determinadas transações).**
- **Verifique a idoneidade da empresa virtual.**
- **Nunca clique em um link que aparece no e-mail, pois pode levar para um clone do site da empresa. Digitar o URL (endereço na rede).**
- **No caso de aplicativos de paquera, marque o primeiro encontro em local público.**
- **Faça sempre atualizações dos softwares.**
- **Nunca pague aos hackers.**
- **Verifique se seu e-mail está nas listas de vazamento de dados na internet.**

rede. Um site gratuito e seguro, criado pelo especialista australiano Troy Hunt, é o Have I Been Pwned (https://haveibeenpwned.com). Embora esteja em inglês, é facilmente utilizável por todos. Basta inserir seu endereço de e-mail e clicar no botão "pwned". O site irá verificar se sua conta está na lista de mais de 1 trilhão que foram hackeadas nos últimos anos e permite também criar uma notificação automática caso apareça em futuros vazamentos de dados. Se for alvo de vazamento, é importante mudar a senha imediatamente em todos os serviços mais utilizados.

Para quem foi atingido pelo vírus, é possível encontrar na internet ferramentas gratuitas de remoção. Elas removem vírus de ransomware (software malicioso) do computador e decifram os arquivos que foram criptografados no ataque. Também informam sobre os tipos de ransomware e mostram como eles são. Alguns exemplos são Alcatraz Locker, Apocalypse, BadBlock, Bart, Crypt888, CrySis, Globe, Legion, NoobCrypt e SZFLocker.

## Atenção aos adolescentes

As crianças de 10 a 14 anos merecem atenção especial dos pais nas redes sociais, na avaliação de Jeroen. "Os adolescentes são preocupantes. Nessa idade, eles costumam ser muito vulneráveis e não entendem que a pessoa do outro lado pode estar mal-intencionada", afirma. Muitas informações no Facebook, por exemplo, servem de orientação a golpistas para descobrir o endereço, parentes, amigos e principais hábitos dos usuários. "O pai pode pensar que o filho está seguro no quarto envolvido com o computador, mas ali pode ser um espaço totalmente inseguro", alerta o professor.

Quanto aos aplicativos de paquera, Jeroen faz um alerta já sabido: o primeiro encontro deve sempre acontecer em locais públicos, pois nunca se sabe se a outra pessoa é real ou virtual. "Alguns aplicativos são conectados ao Facebook, aí fica mais fácil saber se a pessoa está falando a verdade ou fantasiando", diz. Quando possível, é recomendado consultar a página do pretendente.

Entre os golpes cibernéticos preferidos dos criminosos está o do "exame falso". Com posse de informações detalhadas das pessoas internadas em hospitais, obtidas pela internet, os meliantes se passam por médicos, ligam para familiares e alegam situação alarmante, o que faz com que se caia no golpe. Eles costumam dizer aos familiares que o plano de saúde não cobre o procedimento ou demora muito tempo para autorizar. E pedem que os parentes façam uma transferência bancária.

Os dados de saúde são os mais valiosos nos ataques cibernéticos, segundo o fundador da Perallis. Ele lembra o recente ataque no Hospital de Câncer de Barretos (SP), em que cerca de três mil consultas e exames foram suspensos depois que invasores bloquearam os sistemas e pediram resgate em bitcoins, a moeda virtual mais conhecida da internet, para liberar o acesso.

Para alertar a população sobre os riscos de ataques e apresentar medidas preventivas, o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil tem uma cartilha de segurança para a internet (https://cartilha.cert.br). Lá é possível encontrar informações sobre ataques, códigos maliciosos, spam, senhas, criptografia, privacidade, segurança de redes e computadores e em dispositivos móveis, além de extenso glossário de termos do universo tecnológico. O centro adverte que o pagamento do resgate não garante que você conseguirá restabelecer o acesso aos dados, além de encorajar novos ataques de hackers.

# Dicas gerais de segurança

## BACKUP

- Mantenha seus equipamentos atualizados.
- Use apenas programas originais e tenha sempre as versões mais recentes dos programas instalados.
- Instale todas as atualizações disponíveis, principalmente as de segurança.
- Crie um disco de recuperação e tenha por perto, para possíveis emergências.
- Instale um bom antimalware.

## MALWARE

- Mantenha o antivírus atualizado, incluindo o arquivo de assinaturas.
- Atualize o arquivo de assinaturas pela rede, de preferência diariamente.
- Configure o antivírus para verificar, automaticamente, toda e qualquer extensão de arquivo, arquivos anexados aos e-mails, obtidos pela internet e os discos rígidos e as unidades removíveis.
- Verifique sempre os arquivos recebidos, antes de abri-los ou executá-los.

## SPAM

- Evite executar, simultaneamente, diferentes antivírus, porque eles podem entrar em conflito, afetar o desempenho do equipamento e interferir na capacidade de detecção um do outro.
- Crie um disco de emergência de seu antivírus e use-o se desconfiar que o antivírus instalado está desabilitado/comprometido ou que o comportamento do equipamento está estranho.

## SAFETY

- Assegure-se de ter um firewall pessoal instalado e ativo.
- Verifique, periodicamente, os logs do firewall à procura de acessos maliciosos.
- Proteja seus dados, fazendo backups regularmente.
- Nunca recupere um backup se desconfiar que ele contém dados não confiáveis.
- Mantenha os backups desconectados do sistema.
- Não considere que mensagens vindas de conhecidos sejam sempre confiáveis: o campo de remetente do e-mail pode ter sido falsificado ou elas podem ter sido enviadas de contas falsas ou invadidas.
- Antes de acessar um link curto procure usar complementos que permitam visualizar o link de destino.
- Use a conta de administrador apenas quando necessário. Cuidado com extensões ocultas, porque alguns sistemas possuem como configuração padrão ocultar a extensão de tipos de arquivos suspeitos conhecidos.
- Desabilite a autoexecução de mídias removíveis e de arquivos anexados.
- Revise permissões e configurações de segurança.
- Use autenticação de dois fatores.
- Use um bom gerenciador de senhas.
- Use VPN quando estiver em redes WiFi públicas.
- Use criptografia para trocar e-mails confidenciais.
- Proteja o roteador, colocando uma senha forte e atualizando a bios do mesmo.
- Tenha uma boa solução de segurança no PC e no celular.
- Bloqueie o celular (do jeito certo – senha alfanumérica ou leitor biométrico).
- Aprenda a fugir da manipulação da engenharia social.

## TOOLS

## PASSWORD

## PREVENTIVE

## FIREWALL

*Fonte: Glicério Ruas*

# Clicou, gerou rastro e ameaçou a privacidade

Mesmo uma pessoa discreta, avessa a exposições e a redes sociais pode ter a privacidade invadida se tem o hábito de usar a internet, aparelho celular, e-mail e aplicativos de transporte urbano. Endereço, amigos, lista de chamadas telefônicas, hábitos mais comuns, fotos, vídeos, conversas e áudios não pertencem apenas ao indivíduo. Qualquer tipo de informação compartilhada na rede torna-se pública não só para empresas detentoras das tecnologias, como também para outros usuários das plataformas digitais.

E se o seu celular tiver acesso ao microfone, tenha cuidado. Suas conversas podem ser ouvidas mesmo quando ele não estiver conectado. "A privacidade virou artigo de luxo. Abrimos mão dela para ter certa comodidade. É o preço que pagamos, não existe almoço grátis", afirma **Joana Ziller,** pesquisadora do Núcleo de Pesquisa em Conexões Intermidiáticas e professora do Departamento de Comunicação da Universidade Federal de Minas Gerais (UFMG).

Toda ação na rede digital gera um rastro, seja ele consciente ou não. E diferentemente das ações que se dão no ambiente físico e também geram rastros, o ambiente digital tem um comportamento próprio. "Quando preenchemos um formulário on-line, esse rastro é consciente. Já quando a pessoa clica em um link ou curte ou comenta uma mensagem na rede social, provavelmente não sabe que está deixando rastro", observa Joana. Mas está mostrando para o Facebook as temáticas de que gosta e as pessoas que poderiam ser suas amigas.

A entrada em uma página que tenha cookies pode não se associar necessariamente à pessoa que está navegando, mas com certeza ao endereço de IP da máquina que ela está utilizando. "Quando acessamos um portal diretamente, estamos conscientes que deixaremos rastro por ali. Porém, muitos sites abrem diversas outras páginas que contêm propagandas, fazendo com que você deixe suas informações em lugares desconhecidos e sem mesmo notar", afirma **Juan Cabral,** especialista

Daniel Protzner

Fernando Rosenthal

Banco de imagens - Freepik

### *ENTENDA OS RASTROS DIGITAIS*

É um volume expressivo de rastros de ações gerado, monitorado e tratado cotidianamente na internet, constituindo-se em imensos arquivos sobre as atividades e modos de vida. Praticamente todos os softwares hoje levam em consideração esses rastros, que estão sendo apropriados por diversos campos, como vigilância, publicidade, entretenimento e serviços. Eles também vêm sendo valiosa fonte de pesquisa nas ciências humanas e sociais.

em aplicativos, da agência Novos Elementos, focada em internet e marketing digital.

## Perigo nos downloads

Os portais, sites ou aplicativos acessados, diz Juan, sempre guardam informações da pessoa. "Portanto, o ideal é não passar nenhum dado pessoal crucial pela internet como, por exemplo, senhas de banco", alerta. Eles tentam fornecer informações mais personalizadas, por isso, a todo momento, coletam dados dos usuários para cumprir tal objetivo. "Isso acaba comprometendo a privacidade", afirma o especialista. Ele ressalta que as páginas de downloads são as mais perigosas. "Esses sites necessitam de anúncios e, infelizmente, muitos deles contêm links maliciosos que podem gerar diversos problemas para os usuários", observa.

Todas as ações são decodificadas e armazenadas em bancos de dados que viram estatística e retornam em forma de personalização dos resultados nas pesquisas dos buscadores. Significa que, ao percorrerem páginas, emitirem opiniões e interagirem das mais variadas formas, as pessoas imprimem rastros de uma identidade específica e seu estilo.

As redes sociais, como o Facebook, são conhecidas por monitorarem os sites que seus usuários acessam, a fim de personalizar os anúncios. "Todas as informações que aparecem nos feeds são personalizadas devido à interação do usuário", diz Juan. São algoritmos poderosos que permitem ao Facebook escolher as postagens que têm mais possibilidade de "agradar" aos demais usuários.

Os dados são captados sutilmente. Por meio do cruzamento de informações adquiridas, é possível inferir qual seria o comportamento do indivíduo diante de determinada situação. Sendo assim, os rastros implicam não só o controle do passado, mas a indução de um comportamento futuro.

Por isso, quando deixar de usar alguma plataforma, é bom lembrar de excluir perfil e dados inseridos ao longo do período de utilização, pois eles podem evidenciar um momento da vida que ficou no passado e que não reflete a realidade atual, podendo levar a entendimento equivocado da vida pessoal e profissional. E como forma de segurança, é sempre bom manter registro atualizado de sites, portais e aplicativos que utiliza ou tenha utilizado e evitar compartilhar dados em qualquer plataforma.

# WhatsApp fora do ar deixa usuários em polvorosa

O aplicativo WhatsApp é um serviço que, geralmente, é o primeiro a ser checado pela maioria dos usuários antes de dormir e logo ao abrir os olhos pela manhã. A indisponibilidade dele causa revolta e contamina a rotina de mais de 120 milhões de brasileiros. Pois esse foi o cenário ocorrido desde 2015 nos episódios em que a Justiça brasileira colocou o aplicativo fora do ar.

Das quatro decisões, em três foi bloqueado. Em todos os casos, o Facebook, dono do WhatsApp, se negou a conceder informações para investigações criminais, o que levou a Justiça a determinar o corte do serviço. A rebelião dos usuários foi tanta que na terceira ordem judicial, que determinou o bloqueio do aplicativo por 72 horas em todo o país, o grupo de hackers Anonymous Brasil chegou a atacar o site do Tribunal de Justiça de Sergipe (TJ-SE), responsável pela decisão. "Se o WhatsApp ficará bloqueado por 72 horas, assim será também com o site do Tribunal de Justiça de Sergipe, em forma de protesto", informou a mensagem publicada na página do grupo, no Facebook.


Divulgação

O rebuliço imediato é fácil de ser explicado. O aplicativo entrou para a rotina mundial da população e é hoje a forma de envio de mensagens instantâneas mais usada no Brasil. Tem ainda o benefício de oferecer chamadas gratuitas de voz e videochamada para smartphones, além de mensagens de texto, envio de imagens, vídeos e documentos em PDF.

A polêmica ao redor das decisões judiciais contra o aplicativo se arrasta desde então e não há garantias de que novos bloqueios não possam acontecer. A Associação Brasileira de Defesa do Consumidor (Proteste) atua como *Amicus Curiae* (amigos da Corte) na ação que tramita no Supremo Tribunal Federal questionando os bloqueios. Isso significa que a associação intercede no processo com o objetivo de apresentar ao Tribunal sua opinião sobre o debate.

"Lá temos defendido que decisões determinando o bloqueio do aplicativo não encontram amparo no Marco Civil da Internet. Ao contrário, revelam interpretação equivocada do artigo 12 da lei", afirma a advogada **Flávia Lefèvre**, conselheira da Proteste e do Comitê Gestor da Internet no Brasil. Além disso, diz, o bloqueio fere o princípio da proporcionalidade, na medida em que milhões de usuários são impedidos de usar a aplicação, por conta de impasses técnicos relativos a um caso específico de investigação criminal.

## Comunicação digital

Cada vez mais a comunicação das pessoas passa pelo digital, e o aplicativo é a forma usada por muitas famílias e amigos para planejar eventos, a rotina dos filhos e combinar horários. As empresas e profissionais se utilizam também dele para marcar reunião, consultas e falar com os clientes, além de outras finalidades. "O bloqueio do WhastApp causa muitos danos e transtornos a essas pessoas. Mas o principal estrago é em relação à nossa própria democracia em si. O WhatsApp é uma

ferramenta de uso amplo e irrestrito", afirma o advogado **Maurício Brum Esteves**, especialista em propriedade intelectual e também sócio do escritório Silveiro Advogados, em que atua com grande ênfase na área de tecnologia da informação.

Essas decisões judiciais, segundo o advogado, vão contra o princípio da neutralidade da rede, que prevê a necessidade de transmissão, comutação e roteamento de pacotes de dados sem qualquer discriminação. "Principalmente depois do regulamento do decreto nº 8.771/2016, um dos que regulamenta o Marco Civil da Internet e especifica as possibilidades de discriminação do tráfego, ficou mais evidente ainda que medidas como bloquear o WhatsApp importam em violação ao princípio da neutralidade da rede", completa.

Na avaliação dele, os magistrados aprenderam essa via de bloqueio do aplicativo como forma de obter informações facilitadas para investigações criminais. "E como questões envolvendo tecnologia da informação e direito não são ainda de grande debate ou apreciação acadêmica, no Brasil, em comparação com outras temáticas mais populares, os magistrados acabaram descobrindo essa forma facilitada de obter comunicações privadas", diz Maurício. Essas informações passam pelo âmbito digital e acabam deixando rastros, muito mais do que a comunicação feita de forma física, que de repente podem envolver diálogos que não deixam registros. "Hoje em dia, as nossas comunicações deixam registros e cópias e os magistrados evidentemente estão tentando se valer dessa nova possibilidade para fazer as investigações", afirma.

Mas o advogado faz análise que vai além do fato de o bloqueio do WhatsApp violar a neutralidade da rede. "Os magistrados estão exigindo que o aplicativo entregue dados que não são de guarda obrigatória. O Marco Civil exige que comunicações privadas sejam objetos de guarda facultativa e não obrigatória", afirma. Na verdade, diz ele, apenas os registros de acesso referentes à data e à hora de uma determinada aplicação, a partir de um Internet Protocol (IP, o número que o computador ou roteador recebe quando se conecta à internet), são de guarda obrigatória.

Ele esclarece que o regulamento do decreto nº 8.771 trouxe o princípio da retenção mínima de dados, que prevê que os dados de guarda facultativa, ou seja, pessoais e de comunicações privadas, devem ser guardados apenas para atender determinada finalidade e depois serem automaticamente excluídos. Os dados de guarda obrigatória, que são os registros de acesso à aplicação e de conexão, devem ser armazenados pelo período de seis meses para as informações de acesso à aplicação e um ano para os dados de conexão.

No caso do WhatsApp, portanto, Maurício explica que as comunicações privadas são de guarda opcional e o


Ricardo Lages

aplicativo optou por não armazená-las. "A proposta é justamente garantir as informações criptografadas e com segurança. Em resumo, as decisões que determinaram o bloqueio do serviço do WhatsApp ferem, sim, o princípio da neutralidade da rede e o aplicativo não está obrigado a efetuar a guarda de comunicações privadas, visto que é optativo", afirma.

Flávia, da Proteste, ressalta que o uso da criptografia de ponta a ponta na troca de mensagem inviabiliza a entrega do conteúdo das mensagens e, portanto, a empresa pode informar os metadados que se mantêm íntegros apesar da codificação, mas não há como entregar o conteúdo das mensagens. "É importante destacar que o uso da criptografia é estimulado pelo Marco Civil da Internet e pelo decreto que o regulamenta", afirma. Além disso, diz, a lei quis garantir segurança aos usuários da internet, determinando aos provedores de serviços que utilizem as ferramentas existentes, fazendo menção expressa à criptografia.

As regras do jogo devem ser respeitadas de forma unânime, segundo Maurício. "Por enquanto, é que comunicações privadas não são de guarda obrigatória, então os provedores de aplicação não podem ser obrigados a entregar esses dados", afirma. Caso o Parlamento entenda que a lei deve ser alterada, diz ele, aí, sim, os provedores vão ser obrigados a entregar as informações. "Mas não é

o que acontece hoje. E caso um dia sejam obrigados a entregar, teremos um grande déficit democrático", afirma.

Para resolver a polêmica, Flávia defende que o Ministério Público e a polícia atualizem seus arsenais investigativos. "É preciso que não se tornem dependentes da quebra de garantias constitucionais para realizarem seus trabalhos, o que penaliza milhões de brasileiros, para tornarem efetivas suas investigações", afirma.

## *BLOQUEIOS DO APLICATIVO*

### FEVEREIRO DE 2015

**A primeira decisão foi a do juiz Luis Moura Correia, da Central de Inquéritos da Comarca de Teresina, depois que o Facebook, dono do aplicativo, se negou a conceder informações para uma investigação policial. Na ocasião, o aplicativo não chegou a ficar fora do ar.**

### DEZEMBRO DE 2015

**O segundo bloqueio partiu da 1ª Vara Criminal de São Bernardo do Campo e corria em segredo de Justiça. Segundo o Tribunal de Justiça de São Paulo, o WhatsApp não atendeu a uma determinação judicial de julho de 2015 envolvendo uma ação criminal. O aplicativo de mensagens ficou fora do ar por cerca de 14 horas.**

### MAIO DE 2016

**A terceira decisão veio do juiz Marcel Maia Montalvão, da Justiça de Sergipe, que ordenava o bloqueio do WhatsApp em todo o país por 72 horas. O pedido foi feito porque o Facebook não cumpriu uma decisão judicial anterior de compartilhar informações que subsidiariam uma investigação criminal. A operadora que descumprisse a ordem pagaria multa diária de R$ 500 mil.**

### JULHO DE 2016

**O WhatsApp ficou bloqueado no Brasil inteiro por cerca de 24 horas por decisão da Justiça do Rio de Janeiro, também pelos mesmos motivos relacionados acima.**

## *A VERSÃO DO WHATSAPP*

- Não é possível atender às determinações judiciais, pois as mensagens não ficam armazenadas em seus servidores.
- Alguns conteúdos até ficam no banco de dados, quando há falta de conexão do destinatário e as mensagens não são entregues, mas ainda essas mensagens não podem ser lidas por estarem protegidas por forte camada de criptografia.
- A tecnologia usada é a criptografia de ponta a ponta, em que a mensagem é criptografrada na saída da caixa do emissor e apenas decodificada ao chegar ao destinatário.

## *O QUE DIZ O DECRETO 8.771, DE 11 DE MAIO DE 2016*

Regulamenta a lei nº 12.965, de 23 de abril de 2014, para tratar das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, indicar procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, apontar medidas de transparência na requisição de dados cadastrais pela administração pública e estabelecer parâmetros para fiscalização e apuração de infrações.

# Crimes contra a honra lideram violações em ambiente digital

Calúnia, difamação e injúria, os chamados crimes contra a honra, juntamente com a ameaça e o estelionato continuam liderando o ranking dos principais delitos cibernéticos praticados no país. Em Minas Gerais, esse cenário se repete. De janeiro a agosto de 2017, foram registradas 5.465 ameaças contra 4.873 no mesmo período do ano passado, na Delegacia Especializada de Investigações de Crimes Cibernéticos (DEICC), localizada em Belo Horizonte. Os casos de estelionato, nos oito primeiros meses do ano, somaram-se 2.191, contra 1.731 no mesmo período de 2016 *(veja quadro na página 56)*.

O advogado especializado em Direito Digital **Caio César Carvalho Lima** acredita que o preconceito, a intolerância e a falta de percepção sobre o alcance da mensagem contribuem para que esses crimes continuem crescendo. "Somos uma sociedade preconceituosa, tentamos nos esquivar disso. Em uma conversa de bar, um comentário preconceituoso pode ficar restrito a poucas pessoas. A partir do momento em que a pessoa publica um post no Twitter, o alcance passa a ser incalculável. As pessoas perdem o controle da informação. Um tuíte é capaz de alcançar o mundo em poucos segundos, com as curtidas e os compartilhamentos dos usuários", ressalta.

Arquivo pessoal

Da mesma forma que o alcance das redes sociais é imediato, as respostas nesse ambiente são instantâneas. Prova disso foi o linchamento público sofrido pela então estudante de Direito Mayara Petruso, em outubro de 2010, quando postou mensagens preconceituosas e incitando a violência contra nordestinos no perfil dela no Twitter, causando revolta nos usuários dessa rede, que logo se posicionaram a favor dos nordestinos.

Em maio de 2012, ela foi condenada a 1 ano, cinco meses e 15 dias de reclusão pela Justiça de São Paulo. A pena, no entanto, foi convertida em prestação de serviço comunitário e pagamento de multa e indenização de R$ 500. Na época, ela admitiu ter publicado as mensagens como uma reação ao resultado da eleição presidencial, quando a candidata do PT, Dilma Rousseff, venceu em todos os nove estados nordestinos.

Caio observa que o julgamento público foi tão severo, que a moça, que, na época, cursava Direito e era estagiária de um escritório de advocacia de renome, perdeu o estágio, abandonou a faculdade e mudou-se de cidade com medo de represálias. "Acredito que ela não tinha ideia da repercussão que o fato teria", afirma o advogado, que é um dos sócios do Opice Blum Escritório Advogados Associados. Ela foi denunciada pelo Ministério Público com base no artigo 20, § 2º, da lei nº 7.716/89, que trata do crime de discriminação ou preconceito de procedência nacional.

Os tribunais brasileiros estão enfrentando e punindo internautas, crackers e hackers que utilizam a rede mundial de computadores como instrumento para a prática de crimes, levando em consideração a legislação atualmente já existente, bem como a jurisprudência e a doutrina.

*Mensagens publicadas nas mídias sociais podem ser repercutidas, tanto positivamente quanto negativamente, de forma muito rápida*

Cerca de 95% dos delitos cometidos eletronicamente já estão tipificados no Código Penal brasileiro por caracterizar crimes comuns praticados por meio da internet. O restante compreende transgressões que só existem no mundo virtual, como invasão de sistemas, distribuição de vírus eletrônico, cavalos de troia e worm.

## Fraudes eletrônicas

Para o titular da Delegacia Especializada de Investigações de Crimes Cibernéticos (DEICC), Frederico Abelha, a internet não é um campo novo de atuação, mas apenas um novo caminho para a realização de delitos já praticados no mundo real, bastando apenas que as leis sejam adaptadas para os crimes eletrônicos. Hoje é mais acessível adquirir um computador ou um smarthphone. Pessoas com baixo nível de instrução com relação ao funcionamento da internet começam a usá-la e passam a acreditar em tudo o que veem. "O problema está na falta de informação. Muita gente idosa, que fica em casa, com tempo livre, entra nas redes sociais e não tem malícia. A dica é consultar pessoas com mais esclarecimento para ajudar. Embora todo mundo seja vítima em potencial, geralmente pessoas com certo grau de inocência e com baixa instrução são os principais alvos dos criminosos virtuais", afirma o delegado.

Para Caio, há falta de educação também no campo digital. "Sem educação não conseguimos ir muito além. Temos exemplos de pais que não tiveram educação tecnológica e os filhos são os tutores deles. Isso vai desde chamar um táxi no aplicativo, identificar phishing no e-mail a atualizar programa de computador e sistema operacional. A falta de educação digital e a forte disseminação da internet no Brasil, com a inclusão digital para todas as faixas etárias e classes, têm colaborado para o crescimento das fraudes no país", acredita.

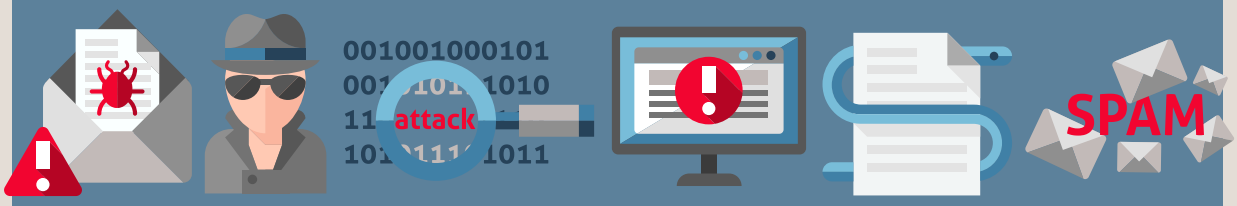
Ele afirma que, nos países desenvolvidos, as crianças têm aulas de programação nas escolas para aprender como funciona o ambiente da internet, mapear os riscos e saber evitá-los. No Brasil, as iniciativas nesse sentido acabam sendo promovidas individualmente. "O Marco Civil da Internet obriga que o Governo tenha como uma de suas metas a inclusão da educação digital na educação básica, mas, infelizmente, o poder público não vem cumprindo essa determinação, mas certamente devemos lutar para melhorar essas questões", afirma Caio.

A formação de profissionais de Direito em Direito Digital também ainda é tímida, já que instituições de ensino superior apresentam o tema como disciplina optativa. Em São Paulo, a faculdade Mackenzie é uma das poucas, senão a única, que a torna obrigatória.

## Privacidade

O Brasil possui leis setoriais de privacidade e proteção de dados pessoais, como o Código de Defesa do Consumidor, a Lei do Cadastro Positivo e o Marco Civil da Internet. No entanto, não há uma lei geral, como na Europa, que a possui desde 1995. "Temos alguns projetos de lei tramitando no Congresso Nacional, sendo três mais relevantes, devendo ser um deles aprovado ainda neste ano ou, no máximo, em 2018. O mais importante deles tem cerca de 60 artigos e todos dispõem sobre privacidade de produção de dados. Com a aprovação, vamos ter um microssistema só para lidar com esse tema", observa Caio.

Em uma sociedade cada vez mais orientada por dados, a lei vem dispor sobre os procedimentos que devem ser considerados quando se fala de tratamento de dados pessoais, referindo-se à coleta, expectativas dos usuários, regras de armazenamento, compartilhamento e exposição dos dados pessoais coletados.




## *Registros de crimes cibernéticos quanto ao meio utilizado*

*janeiro a agosto de 2016 e de 2017*

| | Crimes cibernéticos em Minas Gerais | 2016 | 2017 | Total geral |
|---|---|---|---|---|
| 1 | Ameaça | 4.873 | 5.465 | 10.338 |
| 2 | Estelionato | 1.731 | 2.191 | 3.922 |
| 3 | Difamação | 1.697 | 1.936 | 3.633 |
| 4 | Outras ações de defesa social | 1.098 | 1.341 | 2.439 |
| 5 | Outras infrações contra a pessoa | 828 | 892 | 1.720 |
| 6 | Injúria | 740 | 953 | 1.693 |
| 7 | Calúnia | 617 | 695 | 1.312 |
| 8 | Outras infrações contra o patrimônio | 576 | 666 | 1.242 |
| 9 | Outras denúncias / reclamações / solicitações | 193 | 240 | 433 |
| 10 | Outras infrações / demais leis especiais | 156 | 227 | 383 |
| 11 | Perturbação da tranquilidade | 176 | 181 | 357 |
| 12 | Outras infrações contra dignidade sexual e a família | 134 | 115 | 249 |
| 13 | Perturbação do trabalho ou do sossego alheios | 115 | 90 | 205 |
| 14 | Ingresso ilegal de celular/rádio em estabelecimento prisional | 6 | 122 | 128 |
| 15 | Alteração sem autorização em sistema de informação | 58 | 47 | 105 |
| 16 | Falsidade ideológica | 61 | 44 | 105 |
| 17 | Desobedecimento à ordem judicial (perda/suspensão de direito) | 49 | 50 | 99 |
| 18 | Atrito verbal | 44 | 40 | 84 |
| 19 | Falsa identidade | 50 | 26 | 76 |
| 20 | Constrangimento ilegal | 42 | 33 | 75 |
| 21 | Divulgação meio informação/TV/foto de cena de sexo com criança/adolescente | 30 | 25 | 55 |
| 22 | Inserção de dados falsos em sistemas de informações | 8 | 46 | 54 |
| 23 | Atendimento e denúncia / infrações contra a mulher (violência) | 40 | 11 | 51 |
| 24 | Desacato | 25 | 26 | 51 |
| 25 | Outros crimes | 452 | 532 | 984 |
| **Total Geral** | | **13.799** | **15.994** | **29.793** |

*Fonte: DEICC*

# Dark web e deep web: o lado oculto da internet

Os atos mais sórdidos, repugnantes e abomináveis capazes de serem praticados por um ser humano são divulgados em um ambiente obscuro da internet chamado dark web (web escura), uma fatia pequena da deep web (web profunda), que é mantida escondida. Por conter materiais que envolvem crimes e outros conteúdos mais pesados, capazes de chocar até mesmo profissionais acostumados com práticas hediondas, não pode ser acessada por mecanismos de busca comuns, como o Google Search.

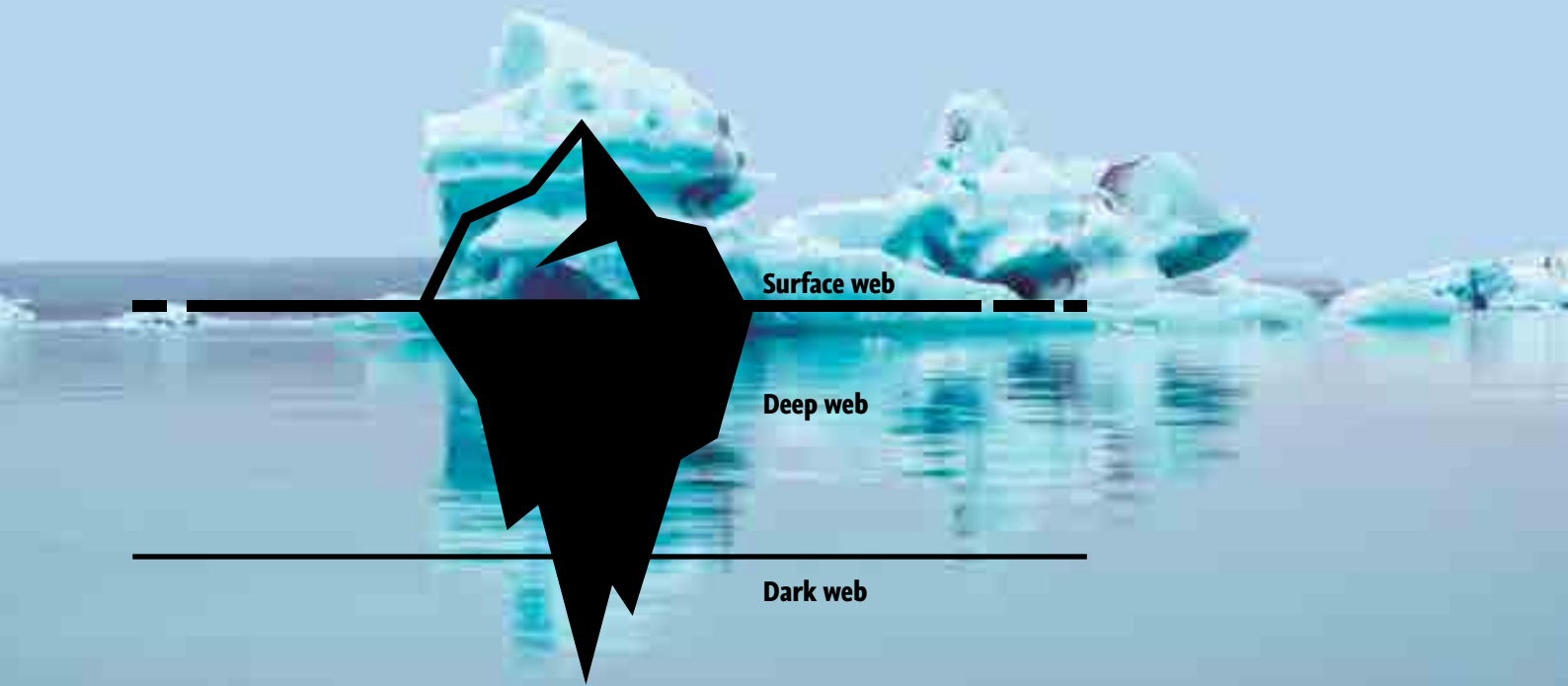
Vídeos de pedofilia e outras práticas sexuais doentias que envolvem torturas, sites em que é possível comprar drogas poderosas, serviços por meio dos quais se contratam pistoleiros para matar alguém, além de tráfico de armas, de órgãos e pessoas. Tudo isso compõe a dark web, localizada em uma fração minúscula quando comparada com os quase 1 bilhão de sites da surface web, ambiente que o usuário acessa para ler artigos, reportagens, fazer pesquisas, enfim, navegar diariamente de forma livre.

Acessar a dark web requer softwares específicos, como o Tor (um dos mais populares, que permite a comunicação entre os sites .onion), e uma série de conhecimentos mais técnicos e de cuidados. A parcela maior da dark web abriga sites antiquados, inúteis e muitas vezes abandonados. Isso acontece porque o Tor passa o tempo todo alterando as rotas de transferência de informação para evitar que dados sejam rastreados. Sendo assim, os criminosos se sentem protegidos do risco de serem pegos facilmente.

O anonimato que ela fornece para o acesso a qualquer conteúdo a torna atraente para ativistas políticos, hackers e criminosos virtuais, além de pessoas que buscam compartilhar conteúdo censurado.

## Mecanismos específicos

Todos os sites, navegadores e sistemas operacionais precisam utilizar protocolos de rede, uma espécie de linguagem comum, para funcionarem. Já a dark web estabelece uma camada de protocolo adicional que o computador não conhece, para garantir o anonimato de quem a usa, tornando os sites incomunicáveis. Certos participantes da rede tornam-se intermediários das conexões dos demais usuários e, com isso, qualquer visita ou acesso fica em nome desses usuários e não em nome do verdadeiro internauta. "É possível quebrar o anonimato da dark web com recursos tecnológicos avançados, monitoramento constante e muito empenho", ressalta o advogado especializado em Direito Digital Caio César Carvalho Lima.



*Criminosos buscam a dark e deep webs para agir de forma livre e anônima*

A instalação de programas espiões vem sendo empregada pelo FBI, após autorização da Justiça para tomar o controle de determinados sites, por meio de um código especial que é colocado na página para tentar contaminar os usuários com vírus e, assim, relatar as informações ao FBI, o que depende de vulnerabilidades no software do possível investigador.

Em Minas Gerais, a Delegacia Especializada de Investigações de Crimes Cibernéticos (DEICC) se dedica à investigação desses criminosos, monitorando esse território obscuro da internet com a ajuda mútua das delegacias de crimes cibernéticos de outros estados da federação. "Temos grupos de WhatsApp de delegados do país inteiro para conversar e trocar informações. O indivíduo que é pedófilo no Rio Grande do Sul pega vídeo aqui em Minas Gerais, na Paraíba, no Amazonas, no exterior, então essas coisas têm que ser monitoradas. Não posso comentar como, mas temos ferramentas possíveis para isso", garante o titular da DEICC, Frederico Abelha.

Na dark web, a pedofilia é o que mais choca. São indivíduos compulsivos, que sentem prazer e são sexualmente atraídos por crianças compartilhando a própria doença. "Há casos em que uma pessoa baixou 60 vídeos de pedofilia em um dia. Para mim, é um dos piores comportamentos que o ser humano pode ter. Há também filmes onde a pessoa mata a outra durante o sexo e aquilo é filmado. Tem de tudo, é o prazer pelo bizarro", comenta.

## Deep web

A deep web consiste em sites "invisíveis", ou seja, páginas que não podem ser detectadas facilmente pelos tradicionais motores de busca, garantindo privacidade e anonimato aos seus navegantes. É formada por um conjunto de sites, fóruns e comunidades que costumam debater temas de caráter ilegal e imoral.

Os endereços eletrônicos que estão na deep web, ao contrário dos disponíveis na internet convencional ou surface web (web da superfície), não são construídos em um formato HTML, justamente para dificultar o acesso. Para isso, é necessária a instalação de programas específicos e o uso de códigos secretos. Ela é 500 vezes maior que a convencional.

De acordo com a legislação brasileira, acessar a deep web não é ilegal, mas o tipo de atividade ou interação que o indivíduo desenvolve nesse ambiente é que pode ser considerado crime.

ENTREVISTA

# Frederico Abelha

Titular da Delegacia Especializada de Investigações de Crimes Cibernéticos (DEICC), professor de Direito Penal e palestrante da Secretaria Nacional de Segurança Pública (Senasp).

Arquivo pessoal

**Os crimes cibernéticos estão crescendo?**

Eles vão aumentar à medida que a internet cresce sem limites. Cada vez mais as pessoas têm acesso à internet, cada vez mais as pessoas vão utilizá-la para tudo. Alguns serviços que eram feitos por indivíduos contratados, hoje são substituídos pela internet. Há 10 anos, a gente ia à agência bancária três, quatro vezes por mês. Agora, quase tudo é possível ser feito pelo computador. Os crimes cibernéticos vão aumentar cada vez mais com a utilização da internet.

**Para tentar frear os crimes cibernéticos, o que o senhor orienta? O cuidado tem que ser individual?**

A principal orientação é se educar sobre internet. Ler, buscar informações com quem sabe mais. Geralmente, pessoas idosas ou mais simples têm dificuldades com tecnologia. Por isso, é importante conversar com quem é mais instruído na área e não fazer nada de impulso. Muitas vezes, promoções mirabolantes de produtos bem abaixo do preço de mercado são enviadas por e-mail. A dica é sempre desconfiar e adotar a máxima de que "o que é bom para ser verdade, geralmente, é mentira". Então, é importante verificar a proporção entre o valor real do produto e o valor ofertado. Não existe milagre! É preciso entender que, muitas vezes, a vítima contribui para esses crimes, porque, na pressa de levar vantagem, acaba caindo no golpe. É bom lembrar que ela também pode ser processada por receptação culposa, porque, pelo valor, a pessoa sabe que o produto é fruto de roubo ou de desvio de carga, ou ela está sendo vítima de um golpe.

> *"Há dez anos, a gente ia à agência bancária três, quatro vezes por mês. Agora, quase tudo é possível ser feito pelo computador. Os crimes cibernéticos vão aumentar cada vez mais com a utilização da internet"*

**Hoje as crianças e os adolescentes acessam as redes sociais cada vez mais cedo, por meio de smarthphones e computadores presenteados pelos próprios pais. Sabemos que existem pessoas perversas que se sentem atraídas sexualmente por menores de idade. O que o senhor recomenda aos pais para que seus filhos não sejam vítimas de pedófilos?**

Educação familiar é uma coisa personalíssima. Não posso ensinar os pais a criarem seus filhos, cada um cria no modelo que entende ser o melhor. O que a gente costuma orientar é ter a senha do menor de idade; acompanhar os acessos; saber exatamente com quem ele está conversando; limitar o número de horas e de acesso e os sites que podem ser visitados; verificar o histórico da conversa; e, principalmente, manter o diálogo aberto. Muitas vezes, a criança ou o adolescente sente que há alguma coisa errada no contato virtual, mas os pais tratam os filhos de uma forma muito severa que não dão abertura para relatarem o que estão sentindo e o que está acontecendo. A pessoa, por exemplo, está sendo compelida a mandar fotos nuas e não tem coragem de chegar para o pai ou para a mãe e falar o que está acontecendo. E pode estar sendo ameaçada, com alguém falando que vai fazer mal a ela ou mesmo matar seus pais, e fica com medo. Por isso, é importante o diálogo aberto, em que se fale de tudo.

## O senhor acredita que o país tem leis suficientes ou é necessário promulgar outras?

O país não precisa de mais leis, mas que elas sejam efetivamente aplicadas. O brasileiro tem mania de fazer lei para tudo. Nos países desenvolvidos, há pouquíssimas leis, mas elas funcionam. A pessoa que foi pega praticando um crime deve ser condenada e pagar por ele. Mas é um problema cultural, é o problema financeiro do país, a situação econômica, a superlotação dos presídios, o abarrotamento do Poder Judiciário, o sucateamento dos órgãos de segurança pública...

## A Lei Carolina Dieckmann está sendo efetivamente aplicada?

Sim, é uma lei que vem sendo utilizada e pune a divulgação de imagens sem autorização e uma série de crimes que vem acontecendo contra a privacidade. O mais importante é a conscientização da população. Depois que foram tiradas fotos íntimas e divulgadas na internet, a pessoa está sujeita a isso. O telefone pode ser furtado, a pessoa pode levar o aparelho para consertar em algum lugar e ter as fotos furtadas. Enfim, é a vítima concorrendo para que o crime aconteça. Se você não quiser que uma foto íntima sua seja vazada, não permita o registro. Muitas vezes, a pessoa chega à delegacia e a foto dela está em dezenas de grupos de WhatsApp, só na capital. Talvez seja possível chegar na primeira pessoa que enviou. A gente tem como alcançar, que isso fique bem claro, mas é importante que as pessoas se preservem, porque, quando viraliza, fica realmente difícil.

## Quem compartilha também pode ser punido?

Sim, também pode ser responsabilizado. Se ficar comprovado que a pessoa está concorrendo para a difamação, para a divulgação de imagens de terceiros, pode ser punida sim. Já indiciamos várias.

## Existem punições previstas para todo crime cibernético?

É muito comum confundi-lo. O crime cibernético nada mais é do que um crime. O mesmo crime praticado no espaço real é praticado no ambiente virtual. Um estelionato, por exemplo, na rua, um golpe do bilhete premiado, por exemplo, é igual na internet. Se você for vítima de ameaça na rua, alguém fala que vai te matar e, na internet, alguém escreve que vai te matar, é o mesmo crime. Há um crime previsto no artigo 154-A, do Código Penal, que é a invasão de dispositivo. Nesse caso, há um tratamento específico, mas, na maioria, é crime previsto na legislação penal.

> *"O crime cibernético nada mais é do que um crime. O mesmo crime praticado no espaço real é praticado no ambiente virtual"*

## Quais são os desafios para atender à demanda da vítima?

Um questionamento recorrente da sociedade é a morosidade nas respostas. Queria ressaltar que a internet é uma ferramenta global e, como tal, muitas empresas fornecedoras de serviços estão fora do país, tanto de vendas como as proprietárias dessas redes socais. O Facebook está nos Estados Unidos; ele comprou o Instagram, que é a segunda rede mais utilizada; o Telegram é do Leste Europeu. O WhatsApp também foi comprado pelo Facebook. De fato, dependemos da cooperação de outros países, o que dificulta um pouco o processo, não quer dizer que inviabiliza, mas dificulta. Existem as proteções da distância, do anonimato, enfim, há uma série de coisas que dificulta. Se a pessoa é vitima de um estelionato e quem está praticando está no Cazaquistão, a chance de a gente chegar até ela é muito pequena. Trabalhamos com transnacionalidade, com coisas que estão fora do nosso país, do nosso alcance, que dependem da legislação de outros países para liberarem uma ordem judicial, por exemplo. De fato, há esse agente dificultador.

## Quais as provas que a vítima precisa reunir para denunciar um crime virtual?

Se for um crime de valor pecuniário, tem que levar à delegacia as comprovações de pagamento, o endereço do site em que foi feita a compra. Se forem crimes contra a honra, apresentar o perfil do Facebook ou do Instagram de quem está praticando aquilo, prints das telas do WhatsApp ou, melhor ainda, o próprio celular para ser periciado para saber a origem dessas mensagens. Vai depender do crime. Se for um ransomware, levar o pedido de resgate. Enfim, o principal é a prova material. Nas capitais, há delegacia especializada em crimes cibernéticos. Se a vítima está no interior, é preciso procurar uma delegacia policial. Em caso de dúvidas na apuração, a DEICC auxilia na rota investigativa a ser traçada.

Arquivo pessoal

**Antônio Ricardo Gomes Leocádio**

*Mestre em Administração e especialista em Novas Tecnologias e Segurança da Informação. Na área de TI há 20 anos, atua no Banco Mercantil na Gerência com enfoque em Segurança e Arquitetura de Sistemas da Informação. Já participou de diversos trabalhos, como: gestão de identidade, segurança em infraestrutura, segurança em transações financeiras e bancárias, certificado digital, arquitetura de sistemas, comunicação segura entre sistemas heterogêneos, perícia forense e análise de ameaças digitais e adequações a frameworks, como COBIT5 e Itil V3. Proferiu palestras em diversos eventos e instituições no Brasil e no exterior.*

# Segurança cibernética, pessoas, empresas e governos. Precisamos muito falar sobre isso

Históricas batalhas, como a de Troia (1200 AC a 1300 AC), nos revelam que o inimigo sempre é ardiloso e busca nos surpreender para alcançar os próprios objetivos. Atualmente essa "surpresa" é chamada de estratégia e, assim como em Troia, a face do ataque não é revelada até que você a perceba, e esse momento pode ser tardio.

O nosso convívio diário com as novas tecnologias, em algum momento, nos remete a questões relativas às proteções digitais, sejam elas estratégias de negócios, dos dados corporativos, de governos, sejam das informações pessoais.

Esse é o mesmo princípio dos ataques digitais atuais, que encontram, no nosso modo de vida amplamente conectado, uma vastidão de possibilidades para intrusão. A diferença é que, nos dias atuais, precisamos lidar com bem mais inimigos simultâneos. Essa necessidade de combater inimigos acabou gerando o termo segurança cibernética.

A segurança cibernética pode ser definida de forma primária, como: segurança da tecnologia da informação contra acesso não intencional ou não autorizado ou alteração ou destruição dos mesmos. O assunto é sério, especialmente se tivermos um viés no setor de serviços, em que as demandas por novos negócios propiciam a comodidade ao invés de segurança. Essas ações ou pensamento corporativo têm evidenciado o gestor de segurança da informação como um aliado, em face das ameaças digitais.

Em um mundo cada vez mais conectado, a segurança cibernética se tornou um pilar estratégico. As estratégias, nos tempos de crise, alavancaram as preocupa-

ções corporativas, chegando a ser discutidas, muitas vezes, no "board" ou conselhos de administração. Todos entendem que qualquer interrupção na sua capacidade de produção, seja física, seja tecnológica, pode ser fatal no atingimento das metas. Portanto, as ameaças digitais acabam sendo vistas com o mesmo viés de riscos das dimensões econômicas, de imagem ou de reputação.

Em sua pesquisa global sobre segurança da informação, em 2016, a empresa Price Water House Coopers (PWC) relata que muitos executivos apontam a questão cibernética como o risco que definirá a nossa geração. Isso se torna mais compreensível quando analisamos e entendemos que os ataques cibernéticos vêm de uma vulnerabilidade já esperada. Creio que, de tanto disseminar notícias negativas, poucos profissionais de TI são capazes de afirmar que seus dispositivos de internet das coisas (IoT) estão seguros e não serão atacados por uma vulnerabilidade conhecida. Veja que esse risco não é exclusivo da segurança da informação, pois o mesmo é inerente e tem como causa raiz a falta de maturidade dos fabricantes de devices IoT em desenvolver produtos seguros. Minha experiência me deixa afirmar que, de maneira geral, esses aparelhos não têm segurança embarcada e se tornam fáceis de infectar.

Tornou-se comum para boa parte dos profissionais de TI, principalmente os que lidam com a parte estruturante de suas instituições, observar as notícias que estão saindo acerca de dados e informações sigilosas expostos. A perda de um determinado arquivo pode parecer algo sem muita importância em um primeiro momento, mas obtê-lo e expor seu conteúdo pode acabar literalmente com seu negócio, por isso diversas empresas trataram de implantar rapidamente sistemas de DLP (Data Loss Prevention).

Ainda sobre a proposta de estar atento e disseminar informações sobre segurança cibernética, o dia 12 de maio de 2017 veio para marcar o calendário da história digital da humanidade. Pela primeira vez, um ataque cibernético de longo alcance paralisou o mundo, afetando inúmeros países. O WannaCry será conhecido como o primeiro ciberataque realizado em larga escala, não que esse tenha sido efetivamente o precursor, mas, sim, por ter sido um dos mais expressivos, sendo noticiado e comentado por pessoas comuns.

## Do que e quando devemos nos proteger?

Para compreender essa pergunta e chegar ao nível adequado de conhecimento, primeiramente governos, executivos e as pessoas comuns precisam entender que não existe uma "solução única", mas, sim, uma sucessão de soluções complementares importantes para a segurança digital.

> ***"Todo funcionário deve ser responsável pelos dados que passam por ele, já que a responsabilidade pela segurança da informação corporativa deve ser de todos, não apenas de uma área específica. Artigos como o 186 e o 187 do Código Civil deveriam ser de conhecimento intrínseco"***

Além disso, digamos que o processo necessita de um conjunto de habilidades que engloba o profissional da área de segurança e seu elevado nível de dedicação no aprendizado de tais estudos e técnicas, sem renegar as questões legais que as envolvem.

Essas habilidades levam a diversos caminhos como as certificações CISSP ou CISM, que visam capacitar profissionais para atuar no mercado profissional, mas vale aqui uma ressalva – as experiências técnicas de certos profissionais são tão importantes quanto o caminho das certificações.

Segundo matéria publicada no site *Valor Econômico* (2016), treinar funcionários se tornou tão essencial quanto saber usar o antivírus. No caso da empresa citada na matéria, o site mostrou que ela está criando, para a segurança digital dos próprios funcionários, a mesma cultura e ciclo de testes que se tem para outros procedimentos, como de evacuação do prédio e combate a incêndio.

Todo funcionário deve ser responsável pelos dados que passam por ele, já que a responsabilidade pela segurança da informação corporativa deve ser de todos, não apenas de uma área específica. Artigos como o 186 e o 187 do Código Civil deveriam ser de conhecimento intrínseco. O fato é que todos os colaboradores precisam estar cientes dos atuais riscos cibernéticos, no entanto,

cabe aos gestores estabelecer as melhores práticas a serem seguidas e criar um programa de educação digital entre os profissionais.

Exposto tais fatos, fica claro que devemos buscar meios e ferramentas para proteger nossas organizações o mais rápido possível. O mundo de fraudes e ciberataques bate à nossa porta a todo momento e, o quanto antes você estiver preparado, melhores serão suas chances.

E as pessoas comuns, como são impactadas pela falta de segurança cibernética?

O mundo de serviços pode ser o primeiro a falhar para a sociedade, levando em poucas horas ao caos. Já imaginou ficarmos sem serviços bancários, serviços alternativos de transporte, etc.? O Brasil já experimentou por força de Justiça ficar 24 horas sem o WhatsApp. Nesse episódio, foi possível identificar o comportamento das pessoas. Muitas delas realizaram conexões imprudentes, expondo-se, assim, a enormes riscos.

Se não bastasse apenas a falta de serviços, os exploradores de falhas em sistemas já começam a avançar sobre as pessoas comuns que utilizam tecnologia. Segundo matéria publicada no site do bitcoin, minerar bitcoin já é mais rentável que tráfego de drogas e armas na Rússia.

Mas como isso é possível? A resposta parece óbvia, mas usuários comuns não são tão ágeis quando se trata de aplicar correções, mesmo recebendo alertas para essa finalidade.

Aqui cabe uma reflexão sobre a nossa profissão. O profissional de TI tem que entender que nós, por muitas vezes, entregamos um produto inacabado e com falhas, e depois disponibilizamos patchs de correção, algo muito contrário ao que ocorre em outras profissões como médicos, engenheiros, etc. Essa falha pode ser a vertente que propiciamos para fragilizarmos pessoas, negócios e governos.

Com o objetivo de explorar essas vulnerabilidades, os fraudadores, profissionais de TI rotulados como hackers ou crackers, agora usam de suas habilidades para ganhar dinheiro fácil. A cada dia, eles inventam uma nova Troia para alcançar seus objetivos. Nos casos mais recentes, fraudadores estão instalando um agente malicioso (endpoint) minerador de criptomoedas, principalmente para bitcoin. O cenário não tem sido nada animador, pois o foco desses agentes maliciosos tem sido os servidores das corporações, que mantêm um alto nível de disponibilidade e recurso de CPU. Esse comportamento é muito divergente se comparado com o dos primeiros anarquistas digitais, que queriam invadir e pichar, ou daqueles que queriam proliferar malwares.

> ***"Para um cenário futuro, vemos que a confiança se torna algo vital para governos e corporações. Portanto, é necessário que se torne um ciclo o processo de redesenhar as soluções de segurança, pois não existem mais fronteiras entre o físico e o lógico"***

## Mas como assegurar o negócio?

É importante observar que a segurança cibernética também já propiciou a criação de novas formas de comércio. O termo "cyber insurance" (seguro cibernético) apareceu com o advento do "cyber security" (segurança cibernética) e vem sendo ofertado às empresas. Mais uma vez a nossa incapacidade de enfrentar a indústria do medo nos remete a endossar esse tipo de serviço.

Investir em um seguro cibernético pode até garantir o risco financeiro, mas não elimina os riscos intangíveis como os da marca e reputação do seu negócio. Casos como o do vazamento de dados da Playstation e HBO não foram objetivados contra o produto fim da empresa, mas a exploração de uma vulnerabilidade tecnológica produziu prejuízos enormes a essas corporações.

## O futuro e a segurança cibernética

Para um cenário futuro vemos que a confiança se torna algo vital para governos e corporações. Portanto, é necessário que se torne um ciclo o processo de redesenhar as soluções de segurança, pois não existem mais fronteiras entre o físico e o lógico. Deve-se buscar as melhores práticas contra os ataques cibernéticos, não se esquecendo que negócios digitais e inovações irão impulsionar novos negócios, que, por sua vez, irão necessitar também de inovações no que tange à proteção. Isso pede que não recuemos e sejamos resilientes com respostas rápidas, tornando o impacto restrito. A avalanche tecnológica continuará de forma cada vez mais acelerada. Será preciso concentrar-se nos riscos e nas pessoas, e não apenas em dados e sistemas.

Arquivo pessoal

# Ataques cibernéticos: mais que uma realidade


**Bruno Moreira Camargos Belo**

*Gerente do Centro de Tratamento de Incidentes e Operações de Segurança (CTIS) da Prodemge. Bacharel em Sistemas de Informação pela Pontifícia Universidade Católica de Minas Gerais (PUC-MG), pós-graduado em Gestão de Segurança da Informação pela Universidade Fumec. Possui cerca de 15 anos de experiência em Segurança da Informação com atuação em gestão de segurança da informação, segurança em perímetro, tratamento de incidentes, auditoria de sistemas, legislação aplicada e projetos de segurança. Associado ao Information Systems Audit and Control Association (Isaca) – entidade com atuação mundial em assuntos relacionados à segurança da informação, governança, riscos, controles, auditoria de sistemas de informação.*


Desde as últimas décadas, as tecnologias da informação e comunicação vêm sofrendo mutações que configuram um ritmo acelerado de evolução, mudando radicalmente o modo como a sociedade se relaciona. O mundo passou a ser uma grande rede que interconecta pessoas e equipamentos envolvidos em um cenário de inovação e desenvolvimento.

O surgimento da internet das coisas ou IoT completa esse mar de tecnologia e permite que itens usados no dia a dia, como eletrodomésticos, TVs, carros, câmeras de vídeo e até maçanetas de porta se conectem à internet e a outros dispositivos, como computadores e smartphones, por exemplo.

Por outro lado, diante desse avanço tecnológico, surgem os ataques cibernéticos, que, no mesmo ritmo, aumentam o número de vítimas, causam grandes prejuízos e trazem enorme preocupação com a proteção da informação e com toda a infraestrutura e sistemas que a suportam.

Os famosos hackers ganharam nova roupagem. Segundo Tuomo Makkonen, consultor de segurança da F-Secure, os hackers ou os cibercriminosos modernos podem ser, grosso modo, divididos em duas categorias:

**1)** Grupos, entidades altamente organizadas;

**2)** Multidão de hackers amadores vinculados, por meio de fóruns ou da dark web (área da internet que não pode ser acessada por meios convencionais e não possui qualquer tipo de controle).

Uma estimativa do Gartner afirma que, até 2020, cerca de 30% das 2 mil maiores empresas globais serão impactadas por grupos de ciberativistas ou cibercriminosos. Para Paulo Pagliusi, diretor da area de Cyber Risk Services da Deloitte, “os ataques estão cada vez mais monetizados, silenciosos, persistentes e avançados”.

## Alguns ciberataques que ganharam publicidade

Diversos ataques cibernéticos ganharam destaque nos últimos anos. No final de 2013, uma das maiores redes varejistas dos Estados Unidos, a Target, foi alvo de uma invasão em que foram roubados nomes, endereços de e-mail, de correspondência, número de telefone e de cartão de crédito de mais de 70 milhões de pessoas. O prejuízo estimado era superior a US$ 250 milhões.

Em dezembro de 2014, um grupo de cibercrimosos intitulados Guardians of Peace roubou cerca de 100 terabytes de dados da Sony Pictures Entertainment, envolvendo usuários e funcionários. Informações estratégicas foram divulgadas em sites como Pastebin e filmes inéditos foram distribuidos gratuitamente para toda a internet. A Sony estimou um prejuízo de US$ 100 milhões.

Em maio de 2017, o mundo se viu diante de um dos maiores ataques cibernéticos da história, provocado por um ransomware conhecido como WannaCry. Por meio da exploração de uma brecha no sistema operacional Microsoft Windows, o malware infectava o equipamento e se propagava pela rede. Ele começou a agir na Espanha e, em poucas horas, já havia sequestrado arquivos de mais de 300 mil computadores em mais de uma centena de países, inclusive no Brasil. Como resgate, a vítima deveria depositar US$ 300 em bitcoin (moeda virtual) em um endereço/conta dos cibercriminosos. Segundo a fabricante de antivírus Avast, o Brasil ficou entre os dez países mais atingidos, sendo o quinto com mais malware detectados.

Outro tipo de ataque que também preocupa as organizações é o de negação de serviços, DDoS (Distributed Denial of Service). A ameaça de ficar 100% off-line já é realidade. Em um período de cinco anos, o número de usuários passará de 3,3 bilhões para 4,6 bilhões, ou seja, 58% da população mundial estará conectada, revela um estudo da Cisco Visual Networking Index (VNI).

Ainda de acordo com esse estudo, o tamanho médio dos ataques DDoS se aproxima de 1.2Gpbs, o que aponta crescimento de 22%, em 2017. Também alerta que a quantidade de ataques DDoS cresceu 172% em 2016, e a previsão é que esse número cresça 2,5 vezes, totalizando 3,1 milhões globalmente até 2021. Quanto maior o número de dispositivos conectados somados a links de dados cada vez mais rápidos, o poder dos ataques de DDoS aumentará de maneira exponencial.

## Investimentos

De acordo com pesquisa desenvolvida pela consultoria Grant Thornton, a perda financeira que os ciberataques trouxeram para empresas entre janeiro de 2016 e janeiro de 2017 está estimada em US$ 280 bilhões. Com isso, os gastos com segurança da informação estão aumentando.

Uma previsão do Gartner, divulgada em agosto deste ano, é que os investimentos mundiais em produtos e serviços de segurança da informação chegarão a US$ 86,4 bilhões em 2017, aumento de 7% em relação a 2016, com previsão de crescimento em 2018 para US$ 93 bilhões. No entanto, as perdas agregadas, consequência dos ataques cibernéticos, somadas a diversos regulamentos rígidos que entrarão em vigor em 2018, forçarão investimento em segurança, correção de vulnerabildades e resposta a incidentes em escala bem maior que a prevista.

## Como se proteger

Ferramentas para ataques cibernéticos podem ser facilmente encontradas na deep web. O surgimento de ameaças avançadas persistentes (APTs) e cibercriminosos com maior expertise é um desafio que todo profissional de segurança da informação encontra para traçar uma estratégia para contenção desses ataques. A força de reação tem início nesses profissionais que ocupam posições estratégicas nas organizações e podem alinhar as necessidades da segurança com o negócio da empresa.

Os códigos de boas práticas já ditam que, inicialmente, deve ser estabelecida uma política de conscientização sobre segurança que englobe todos – alta gestão, funcionários, clientes e fornecedores, seguida da implantação de processos e medidas preventivas ou corretivas que abranja todo o parque tecnológico.

Para ter visibilidade dos eventos de segurança, deve ser implantado um sistema de monitoramento para identificar ataques ou tentativas de exploração de alguma falha ou vulnerabilidade. É muito importante ter conhecimento daquilo que está acontecendo para que ações sejam tomadas rapidamente e o tempo de resposta a um incidente seja o menor possível. Processos automatizados contribuem muito para essa visibilidade.

O conceito de defesa em profundidade (defense in-depth) não deve ser descartado. Uma boa defesa de perímetro, somada ao monitoramento do tráfego lícito e comportamento da infraestrutura, sistemas e usuários, pode ser uma boa estratégia para prevenir contra ataques.

Segundo Konopacki, do ITS Rio, "os criminosos costumavam fazer um ataque destrutivo, mas sem foco. Hoje eles usam novas táticas para enganar as soluções de segurança das empresas e chegam a ficar meses estudando o ambiente antes de atacar. Ao investir em ferramentas de monitoramento, você identifica o ataque no começo e ganha tempo para agir."

Marcus Santiago

# Cibersegurança: qual o risco mundial?


## Eduardo Honorato

*Líder de Negócios em Cybersegurança na Munio Security. Mais de 20 anos de experiência internacional em consultoria em tecnologia da informação, gerenciamento de risco de informação, conformidade, vendas e desenvolvimento de negócios com especialização em segurança cibernética. Seu foco de atuação está voltado para soluções de Application Security, industrial Cyber Security, SAP Security, além da criação de CSIRTs.*


Este poderia ser mais um artigo comum falando de cibersegurança, tecnologias de proteção, dentre outros pontos tecnológicos. Porém, ao analisar com maior detalhe o relatório de riscos do Fórum Econômico Mundial (WEF, em inglês) – *The Global Risks Report 2017 – 12th Edition*, que analisa todos os riscos mundiais, desde crise de água e comida, crises fiscais, desastres naturais a ataques terroristas, decidi partir para entender o tamanho do problema sobre a cibersegurança.

O relatório mostra que ciberataques aparecem em uma posição de destaque muito próximo de ataques terroristas. É uma informação interessante e preocupante, pois muito se fala e se investe em ataques terroristas e pouco sobre ciberataques.

Mas qual a razão? Poucos investimentos? Poucas pessoas?

Vamos entender com os ataques mundiais de maio e junho de 2017.

Dois significativos ataques cibernéticos aconteceram no mundo, com pouco mais de um mês de diferença entre um ataque e outro, em maio e junho de 2017. No WannaCry, em maio, mais de 150 países sofreram as consequências (e prejuízos), totalizando cerca de 200 mil vítimas, segundo a Europol. No Brasil, diversos órgãos e entidades foram afetados.

Já o de junho, causado pelo ransomware Petya, utilizou as mesmas vulnerabilidades do WannaCry e fez vítimas em diversos países, como Ucrânia, Dinamarca, França, Espanha, Rússia, e também no Brasil.

O cenário assusta, mas o que esses dois megaciberataques nos trazem de lição?

A mais importante delas é que é preciso olhar para sua corporação e avaliar o que foi feito no último mês para aumentar a segurança dos dados e impedir um ataque de hacker.

Está claro que os mecanismos de proteção dos dados adotados pelas organizações são frágeis. E isso faz com que seja fundamental investir corretamente na estratégia de segurança da informação da empresa.

As companhias que estão sendo alvo desse novo ataque cibernético são exatamente aquelas que continuam sem investir em gestão de vulnerabilidade, correção de patches e visibilidade interna. É mais comum do que parece os executivos acharem que como não foram infectados da última vez, estarão livres. E isso não é verdade. Quem continuar sem tomar as medidas de segurança digital necessárias terá uma grande chance de ser atacado ou infectado.

Os hackers sabem da deficiência das empresas em aprimorarem seus sistemas de segurança da informação. No Brasil, precisamos que as empresas melhorem sua maturidade em relação à proteção dos dados.

O que vemos é que os dados corporativos estão sendo expostos de maneira errada pelas organizações. Muitas empresas preocupam-se com a disponibilidade das informações, mas se esquecem da confiabilidade e da integridade dos dados.

Por isso, é preciso fazer uma classificação correta dos dados para que eles fiquem menos expostos. Nesse ponto, entender o valor da informação é essencial para o negócio. As equipes precisam ter maturidade e conhecimento das melhores práticas de segurança da informação e atuar de forma diligente para evitar que a história se repita. O tripé de segurança – processo, pessoa (cultura) e tecnologia – tem que funcionar muito bem. Qualquer falha ou falta de atenção ou priorização em um desses certamente pode gerar o incidente.

A melhor maneira de prevenir incidentes desse porte é com o uso de sistemas de tecnologia atualizados e uma equipe de serviço gerenciado atuando de forma constante e proativa. Imprimir inteligência no processo de segurança é o caminho para prevenir incidentes e ter uma resposta rápida para diminuir a janela de exposição, se ocorrerem.

Zerar a quantidade de ataques ou vulnerabilidades, certamente, é algo utópico. Sendo assim, ter uma política para identificar quais são as vulnerabilidades e estar atento aos ataques são atitudes que minimizam drasticamente a possibilidade de incidente. E isso não se resume à infraestrutura, mas também aos sistemas. Sistemas têm sido desenvolvidos com muitas falhas de segurança. É importante pensar em desenvolvimento seguro.

Para tanto, é necessário ter boas políticas de segurança preestabelecidas, como gestão de vulnerabilidade, análise de impacto ao negócio, testes de invasão recorrentes, plano de continuidade, entre outros.

Agora voltamos ao relatório do Fórum Econômico Mundial, que cita três grandes riscos envolvendo segurança, sendo:

- Desagregação da infraestrutura de informação crítica e redes;
- Ciberataques de grande escala;
- Incidente massivo de fraude ou roubo de dados.

| | | |
|---|---|---|
| | **Crises de água** | Um declínio significativo na qualidade e quantidade disponíveis de água fresca, resultando em efeitos prejudiciais para a saúde humana e/ou atividade econômica. |
| **Riscos Tecnológicos** | **Consequências adversas dos avanços tecnológicos** | Consequências adversas previstas ou não intencionais de avanços tecnológicos como inteligência artificial, geoengenharia e biologia sintética causando danos humanos, ambiental e econômico. |
| | **Desagregação da infraestrutura de informação crítica e redes** | Dependência cibernética que aumenta a vulnerabilidade à interrupção de infraestrutura de informação crítica (por exemplo, internet, satélites, etc.) e redes, causando perturbações generalizadas. |
| | **Ciberataques de grande escala** | Ciberataques em grande escala ou malware que causam grandes danos econômicos, tensões geopolíticas ou perda de confiança na internet. |
| | **Incidente maciço de fraude/ roubo de dados** | Exploração injustificada de dados privados ou oficiais em uma escala sem precedentes. |

*Fonte: The Global Risks Report 2017 - 12th Edition, pág 62*

Hoje em dia, pessoas, empresas e governos dependem muito de infraestrutura tecnológica, tornando-a muito crítica para continuidade de negócios e governos. Portanto, o relatório lista como risco mundial muito alto um possível colapso desse sistema, pois tem a exploração de sua vulnerabilidade muito acentuada. Roubo ou fraude de informação também são citados no documento. Mas o que fazer na prática para manter uma boa cibersegurança?

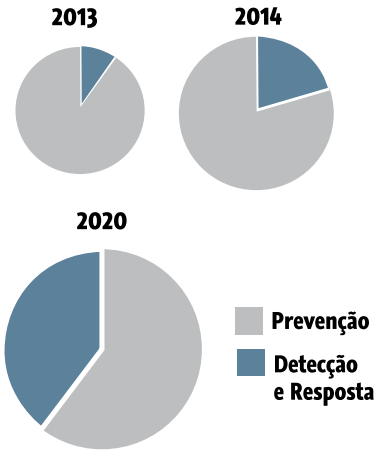
Ainda no relatório, recordamos que cibersegurança está bem próximo de ataques terroristas. E como governos mitigam ataques? Fazendo controle de detecção e resposta, investigação. Governos fazem um bom trabalho de inteligência e, com isso, conseguem mitigar muitos ataques.

E como fazer isso no mundo ciber?

O estudo da Gartner *Shift Cybersecurity Investment to Detection and Response* afirma que, até 2020, 60% dos orçamentos de segurança da informação da empresa serão alocados para abordagens rápidas de detecção e resposta, ante 20% em 2015. (Figura 1)

Esse estudo mostra aumento considerável nos investimentos de detecção e resposta a incidentes de segurança frente aos investimentos de prevenção. Isso quer dizer que investimento em processos para ter um Security Operation Center (SOC) se faz necessário. Estar

**Figura 1**
**Orçamento de TI**




atento a todos os incidentes de segurança é extremamente importante. Com isso, dá-se início a uma investigação de segurança mais eficiente.

Mais do que ter um produto fazendo a proteção, é importante estar com os processos bem definidos do SOC, já que muitos começam comprando equipamento ou softwares sem antes pensar no processo.

A SANS lançou o documento *Building a World-Class Security Operations Center: A Roadmap*, que mostra como construir um SOC "World-Class" ou um SOC em camadas (Figura 2) e ressalta que pessoas, processos e

**Figura2**

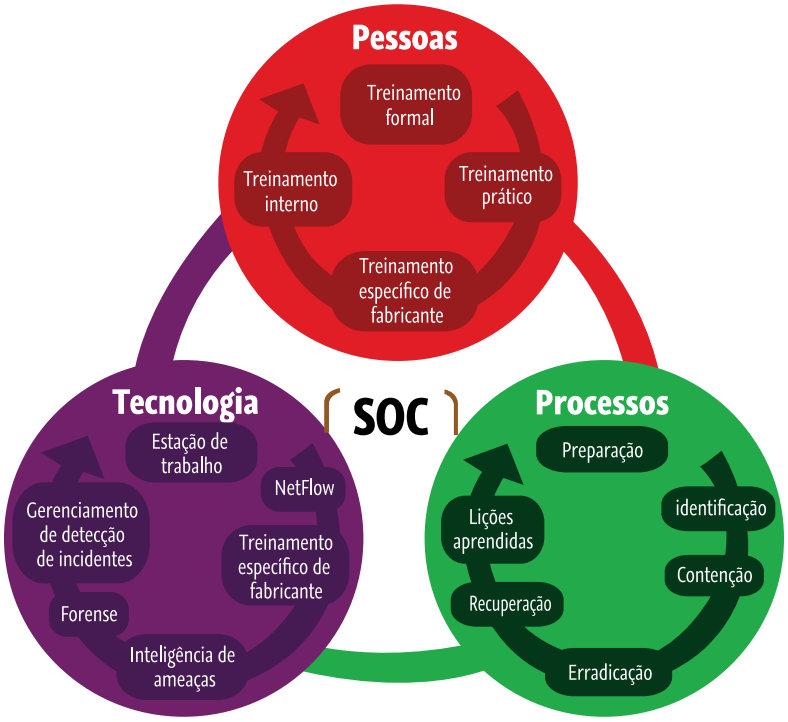
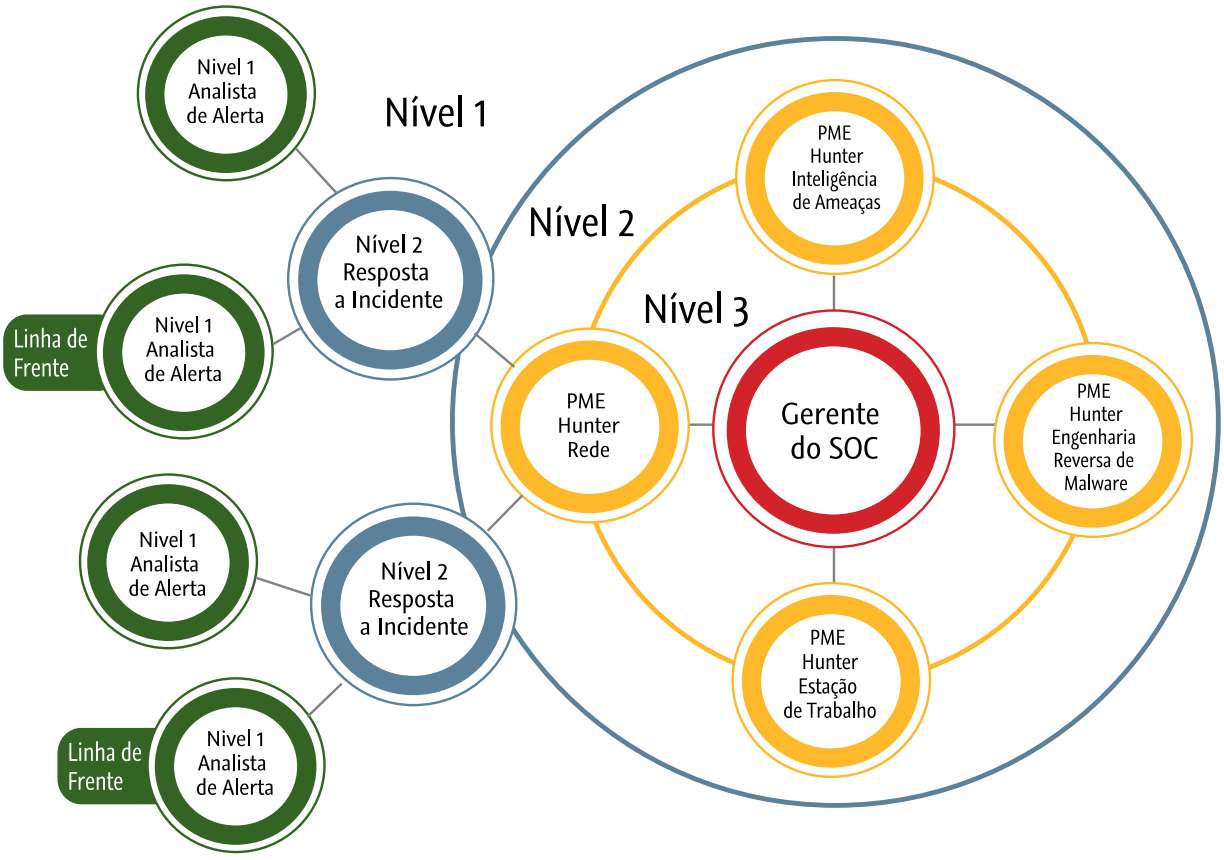


**Figura 3**




tecnologia são realmente importantes para se ter um bom SOC.

A segurança, normalmente, é reativa em mais uma comparação com o terrorismo: quando acontece um ataque, reações imediatas ocorrem. Assim também é na segurança da informação. O propósito é mitigar incidentes. Como fazer isso? Como no terrorismo, threat intelligence ou inteligência de ameaças, somente com inteligência se tem proatividade na segurança da informação. Isso resulta em muita pesquisa e controle de vulnerabilidade e ameaças.

Pensando nisso, a SANS, no seu documento, sugere o seguinte organograma do SOC:

Um SOC organizado em 3 camadas, sendo:

- **Nível 1:** onde ficarão os analistas que estarão de olho nos alertas de segurança;
- **Nível 2:** analistas que cuidam do plano de resposta a incidente e iniciam a resposta;
- **Nível 3:** os hunters ou caçadores. Analistas muito especialistas que farão o threat intelligence, procurando por problemas de vulnerabilidade e ameaças.

Isso fará com que os incidentes de segurança da informação sejam melhor detectados e, assim, com boas respostas. O threat intelligence vai ajudar a não ter maiores incidentes de segurança, antecipando-se a problemas.

Precisamos estar atentos a essas questões. Não saber se está sendo atacado nem de onde vem o ataque é muito prejudicial à estratégia de segurança da informação. Vejam-se os dados do relatório da Microsoft, *The Microsoft Security Intelligence Report*, de 2016.

O Brasil sofre, aproximadamente, três vezes a média mundial de ataques. Portanto, nós, brasileiros, deve-

**Ataques cibernéticos mais comuns no mundo**

| Categoria | No mundo | Estados Unidos | Brasil | China | Rússia | França | Alemanha | Reino Unido | Itália | Canadá | Japão |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Modificação de Navegador | 7.6% | 9.1% | 11.8% | 0.6% | 7.0% | 14.3% | 8.7% | 10.9% | 15.3% | 11.3% | 4.2% |
| Trojans | 7.1% | 4.2% | 12.7% | 10.2% | 20.8% | 5.7% | 4.3% | 4.4% | 7.0% | 5.1% | 1.5% |
| Worms | 3.3% | 0.6% | 8.9% | 5.6% | 4.6% | 1.9% | 1.1% | 0.8% | 3.9% | 0.6% | 0.7% |
| Pacote de Software | 3.1% | 1.7% | 1.5% | 0.2% | 0.5% | 2.2% | 0.9% | 2.3% | 2.5% | 2.5% | 0.5% |
| Downloaders & Droppers | 2.2% | 2.3% | 6.5% | 3.2% | 6.6% | 2.8% | 1.5% | 3.2% | 3.1% | 3.3% | 0.4% |
| Ofuscadores e Injetores | 1.7% | 1.0% | 5.3% | 5.2% | 7.3% | 1.9% | 1.6% | 1.7% | 2.8% | 1.6% | 0.6% |
| Adware | 1.6% | 4.5% | 7.1% | 0.2% | 5.2% | 7.8% | 4.1% | 4.7% | 7.2% | 5.3% | 2.0% |
| Explorações | 1.4% | 3.4% | 2.4% | 1.7% | 1.3% | 2.5% | 3.2% | 4.4% | 4.3% | 5.7% | 3.2% |
| Vírus | 1.1% | 0.4% | 2.2% | 7.4% | 1.5% | 0.4% | 0.3% | 0.3% | 0.8% | 0.4% | 0.2% |
| Outro | 0.6% | 0.9% | 0.3% | 1.2% | 0.3% | 0.5% | 0.5% | 0.6% | 0.7% | 1.5% | 0.2% |
| Backdoors | 0.5% | 0.7% | 1.4% | 1.8% | 2.0% | 0.9% | 0.6% | 0.9% | 1.0% | 0.7% | 0.3% |
| Randsomware | 0.3% | 0.6% | 0.5% | 0.0% | 0.6% | 0.7% | 0.6% | 0.4% | 1.4% | 0.7% | 0.4% |
| Ladrões de Senha e Ferramenta de Monitoramento | 0.2% | 0.4% | 1.0% | 0.5% | 0.8% | 0.3% | 0.4% | 0.4% | 0.6% | 0.6% | 0.3% |

mos mais do que nunca, além de nos proteger, saber de que nos proteger.

A cibersegurança corre um risco muito alto no mundo e no Brasil. Está na hora de olhar para a segurança da informação com atenção e prioridade. A melhor forma de não ser a próxima vítima é se protegendo contra possíveis novos ataques cibernéticos e com bons processos, boas pessoas e boa tecnologia. É preciso manter-se livre de vulnerabilidades e, principalmente, saber detectar o incidente de segurança e responder-lhe.

Arquivo pessoal

# O dilema da proteção de informação nas organizações


**Gilmar Ribeiro**

*Sócio-proprietário e consultor sênior na GPR – Governança e Segurança da Informação. Membro atuante do Comitê CB21 da Associação Brasileira de Normas Técnicas (ABNT). Nesse grupo, coordenou o projeto de desenvolvimento da primeira norma brasileira sobre segurança da informação, a NBR 16.167 – Diretrizes para classificação, rotulação e tratamento da informação. Atualmente, trabalha em um projeto de governança e segurança da informação na Diretoria de Automação da Vale, em Carajás. Formado em Engenharia Industrial Elétrica pela Pontifícia Universidade Católica de Minas Gerais (PUC-MG), pós-graduado em Gestão Empresarial pela Universidade Federal de Minas Gerais (UFMG) e especializado em Engenharia de Qualidade com o título de CQE pela American Society for Quality. Possui certificação ITIL e é auditor ISO27001.*


## O problema

O tratamento inadequado das informações é um problema cada vez mais comum nas organizações e tem gerado perdas consideráveis. Mesmo assim, a maioria das empresas não está preparada para evitar que os funcionários, prestadores de serviço ou mesmo clientes façam cópias e acessos indevidos às informações.

No Brasil, 62% dos profissionais que mudam de emprego levam consigo dados corporativos confidenciais, aponta um levantamento da Symantec, empresa especializada em segurança da informação. Dos entrevistados que admitiram quebrar o sigilo da empresa, 56% disseram que pretendiam usar os dados em uma nova companhia. O porcentual é superior à média dos outros cinco países analisados pela pesquisa, onde 40% dos empregados se acham donos da informação produzida nas empresas. Ainda assim, apenas 33% das companhias dizem tomar alguma atitude quando as políticas internas de sigilo são contrariadas.

A Symantec ouviu 3,3 mil profissionais de Brasil, Estados Unidos, Reino Unido, França, China e Coreia. Os resultados do levantamento mostram que muitos funcionários não só acham que é aceitável levar e usar as informações quando deixam uma empresa, mas também acreditam que as organizações não se importam.

Em termos de estatísticas de vazamentos, recordes foram quebrados em 2016, um depois do outro, de acordo com matéria publicada no g1.globo.com. Em maio, um vazamento do LinkedIn, que se acreditava estar limitado a 6,5 milhões de usuários, ressurgiu com dados de 167 milhões de cadastros.

O Brasil também não escapou de vazamentos. Uma brecha nos sites Ingresso.com e da Samsung deixou despro-

tegidos os dados de clientes, enquanto uma pasta aberta expôs milhões de gravações de chamadas de um call center com atendentes que diziam representar a Claro e a Net (a empresa alegou "desconhecer o caso").

## Preparando o terreno

Nesse contexto, a demanda por proteção de informações é uma tendência crescente nas organizações. Várias empresas, preocupadas com sabotagem, vazamento e acesso indevido às informações críticas e com os prejuízos que possam sofrer, estão partindo para o desenvolvimento de projetos de proteção contra vazamento de informações, utilizando as famosas soluções de Data Loss Prevention (DLP).

Muitas dessas empresas, em alguns casos motivadas pela reação à ocorrência de um incidente e tentando responder de forma rápida para minimizar o impacto em sua reputação ou estancar o problema, cometem grande equívoco de estratégia, buscando imediatamente a implantação de soluções tecnológicas sem se preocuparem com os pilares de um projeto bem estruturado, ou seja, a definição de um processo de proteção de informações e, ainda mais importante, a determinação de quais informações desejam ou realmente precisam proteger.

Para evitar esses problemas, algumas questões devem ser respondidas e resolvidas, para que o projeto tenha sucesso. São elas:

- As informações da empresa e a forma adequada de tratá-las são de conhecimento dos colaboradores?
- Existe um processo de classificação da informação formalmente implantado na organização?
- Existe um inventário de informações mapeado e documentado de acordo com o processo de classificação?
- Os proprietários das informações estão definidos?
- As responsabilidades de todos os envolvidos com as informações estão definidas e atribuídas?
- O ciclo de vida da informação está definido?
- A temporalidade das informações, de acordo com seu ciclo de vida, foi identificada?
- A política e os critérios para concessão de acesso às informações foram definidos?
- Foram definidos os cenários de risco e uso das informações e as regras de tratamento?
- Existe um processo disciplinar pactuado e de conhecimento de todos os colaboradores, visando tratar eventuais desvios ou incidentes comportamentais pelo não cumprimento das regras definidas?
- É desenvolvido um processo de conscientização e cultura em segurança da informação?

De posse dessas informações, a empresa estará em plenas condições de atender aos requisitos fundamentais necessários para tratar adequadamente as informações, abrindo caminho para o desenho de um processo de proteção de informações e, posteriormente, implantar uma ferramenta de DLP com sucesso.

## Desenvolvendo o processo

Muitas empresas ainda convivem com a ideia de que as pessoas são "do bem", de que os processos e fluxos de informações estão corretos e sem falha e que ninguém está interessado nas informações delas.

Na prática, sabemos que não é bem assim! Existem, sim, profissionais "do mal", concorrentes que estão interessados nas informações estratégicas, processos inexistentes ou desenhados de forma incorreta, colaboradores insatisfeitos, atacantes e/ou adversários da rede mundial, dentre outros. Soma-se a isso o aumento considerável de complexidade do cenário de proteção, devido aos avanços tecnológicos que geram perímetros às vezes imperceptíveis ou até mesmo fora de domínio das empresas, em função de novas tecnologias como mobilidade e cloud.

Nesse cenário, a melhoria contínua nos controles de segurança da informação tem que ser uma realidade no dia a dia das organizações. Dessa forma, o ponto de partida para o desenho do processo de proteção é verificar se os pré-requisitos fundamentais foram atendidos, a saber:

- O conhecimento do que precisa ser protegido;
- A identificação dos proprietários dos ativos a serem protegidos;
- Os atores envolvidos nos processos e ativos a serem protegidos;
- O real valor de cada informação, definindo seu grau de sensibilidade;
- Os cenários que envolvem essas informações;
- A definição dos critérios de acesso e grupos de acesso;

- A identificação dos riscos envolvidos.

Atendidos esses requisitos, cria-se uma condição favorável para desenhar o processo de proteção de informação da empresa. O próximo passo será definir os papéis e as responsabilidades, pois, dependendo dessa definição, o fluxo do processo será afetado.

Algumas questões importantes a serem respondidas nessa fase são:

- Quem será o responsável pelo processo de proteção de informações?
- Qual será o papel das áreas de negócio que são, na verdade, os proprietários das informações a serem protegidas?
- Qual será o papel da área de segurança da informação?
- As áreas de Auditoria, Jurídico e RH foram envolvidas?
- Qual será o papel dos gestores da empresa no processo?
- Quem será o responsável pela criação e manutenção das regras de proteção nas ferramentas DLP?
- Quem será o responsável pela análise e avaliação em relação à criação de regras?
- Quem será o responsável por operar o dia a dia das regras de negócio, na solução DLP? Elas foram formalizadas pelos responsáveis das áreas de negócio?
- As áreas de negócio onde o DLP será implantado foram capacitadas e estão comprometidas com o processo?
- Quem será responsável por tratar os incidentes?
- Quem dará suporte ao tratamento dos incidentes?
- O que fazer com os incidentes comportamentais ou de desvio de conduta?
- Existirá um Comitê de Conformidade para tratar os casos críticos envolvendo incidentes de segurança considerados comportamentais, em especial, os relacionados a fraudes e a vazamento de informações?
- Quais as lições aprendidas para melhoria dos processos de negócio em risco?

Uma dica importante ao desenvolver o processo de proteção é considerar o desenho de fluxos independentes:

- Um fluxo envolvendo a criação das regras com as seguintes atividades: solicitação/manutenção de regras, análise da solicitação, criação, teste, validação e implantação das regras de proteção na ferramenta DLP;
- O segundo fluxo deve contemplar a gestão e operação de rotina, dos incidentes gerados pela solução de DLP, envolvendo a avaliação e o tratamento dos incidentes gerados a partir das regras criadas.

A divisão do processo em dois fluxos distintos ajuda, consideravelmente, o gerenciamento, a operação e o suporte ao processo de proteção e permite que os papéis fiquem claramente definidos.

Outro fator fundamental é a documentação formal do processo que, além de padronizar e servir de material de treinamento, fornece estrutura básica para apoio à conformidade legal. Nesse aspecto, é fundamental documentar os requisitos de inviolabilidade e unicidade dos registros, o controle de acesso ao ambiente e a formalização sobre o direito da empresa em monitorar os ativos de TI. Uma boa prática é alinhar o processo de comunicação ao Código de Ética, à Política de Segurança e à Cartilha de Segurança da Informação da empresa.

É importante também reforçar que o processo de capacitação das áreas de negócio em que o DLP for implantado não consiste somente em prevenir contra fraude ou vazamento de informação. O DLP ajuda as empresas a descobrirem fluxos de informações inseguros ou mal desenhados, permitindo a melhoria contínua. Além disso, o processo de proteção de informação apoia a classificação e o tratamento da informação e o desenvolvimento da cultura em segurança da informação nas empresas. Quando o processo de proteção está bem desenhado, padronizado e definido na organização, o uso de controles de conteúdo torna-se um aliado, e não um espião.

Ah! Ia me esquecendo de um detalhe. E quanto à ferramenta DLP?

Bom, vou falar o óbvio. Existem excelentes ferramentas no mercado. Deve-se fazer uma prova de conceito em seu ambiente e avaliar a adequação à infraestrutura da empresa e o custo x benefício do projeto. Assim, será possível identificar a ferramenta mais indicada para a real situação e orçamento da empresa. Mas fique tranquilo! Estando com o dever de casa pronto, certamente a ferramenta será o menor dos problemas. Quando a estrada está bem pavimentada, não importa o veículo!

Arquivo pessoal

# Chuva de dados


## Gustavo Padovani

*Formado em Jornalismo pela Universidade Estadual de São Paulo (Unesp), mestre em Imagem e Som pela Universidade Federal de São Carlos (UFSCar) e especialista em Gestão em Marketing pela Faculdade Getúlio Vargas (FGV). Professor no curso de Imagem e Som da UFSCar e na Pós-Graduação em Administração da Fundação Getúlio Vargas / UniSEB - Ribeirão Preto. Participa do Grupo de Pesquisa em Mídias Interativas em Imagem e Som (GEMInIS) e da rede de pesquisadores Obitel Brasil. Atuou por quatro anos na produção de conteúdo e estratégias de marketing nas redes para o Hospital de Câncer de Barretos. Criador da Fubá Mídia: uma rede responsável por prestar consultoria, criar soluções e executar projetos de comunicação e marketing estratégico para empresas, organizações não governamentais (ONGs) e outros.*


Quando a noção de computação pervasiva foi criada, na década de 1990, por teóricos como Mark Wiser, havia o intento de explicar como, aos poucos, a evolução máxima da tecnologia teria uma penetração tão intensa em nosso cotidiano, que não haveria a necessidade de a enxergarmos. Porém, como toda descoberta tecnológica, leva um tempo de maturação para que o mercado e a ciência cheguem a um estágio de demandas e ofertas exequíveis – período esse que o autor Jeremy Kamp define como "platô de produtividade". Passadas quase duas décadas, esse conceito já é uma realidade, uma vez que estamos cercados por dispositivos móveis vestíveis (werables) e geolocalizáveis – os representantes da chamada internet das coisas – que nos ajudam a executar, gerir e capitalizar milhares de informações.

Em um último estudo, realizado pela Business Software Alliance (BSA) e publicado em 2015, foi constatado que o mundo produz cerca de 2,5 quintilhões de bytes todos os dias. Todos esses dados servem para ilustrar não somente a dimensão que temos como produtores, consumidores e replicadores de dados, mas também como os próprios objetos tecnológicos capturam nossos dados e se comunicam autonomamente entre si. É esse tipo de ação integrada que nos avisa que um voo agendado pode atrasar ou anuncia lugares para comer que surgem no celular perto do horário do almoço. A internet, muito mais do que tornar as distâncias do mundo menos longínquas (materializando o conceito de "aldeia global"), possibilitou nos conectarmos mais ainda com o nosso redor e criarmos cidades sencientes, ou seja, espaços sensíveis que pensam, monitoram e respondem ao nosso comportamento.

Outro grande catalisador da produção de dados são redes sociais como Facebook, Twitter, Instagram e WhatsApp,

pois seus modelos de negócios são baseados no monitoramento e na venda de dados que os usuários criam por meio de textos, fotos, vídeos, preenchimento de informações, buscas e links. Tudo isso se tornou um dos grandes motores da economia. A investidora Mary Meeker, da Kleiner Perkins Caufield & Byers, por exemplo, declarou que o software de reconhecimento de voz do Google nos celulares Android consegue captar 95% das palavras ditas próximas ao telefone. Esse dado faz sentido quando refletimos sobre nossa própria experiência de uso nas redes: quantas vezes um assunto conversado com amigos e familiares aparece imediatamente na timeline de nossas redes sociais?

Embora muitas plataformas aleguem sua segurança, ao participar delas, concordamos com seus termos de usos e condições. Logo, é difícil dizer quando essas funções estão ligadas e quão vulneráveis estamos com esses dispositivos. Em uma célebre foto divulgada em setembro de 2016, Mark Zuckerberg, o próprio CEO do Facebook, aparece em frente ao seu laptop trabalhando com câmera e microfone tampados com fitas adesivas – o que diz muito sobre o quanto ninguém está imune.

## Vigilância e (auto)controle nas redes

A ideia de ser vigiado sem perceber foi materializada no final do século XVIII no conceito construído pelo jurista inglês Jeremy Bentham ao criar o panóptico: um projeto de prisão modelada para que todos os prisioneiros sejam observados por alguém sem saberem se estão ou não sendo vigiados. Sua força simbólica foi utilizada por Michel Foucault para representar os pensamentos sociais de uma sociedade disciplinar que procurava alocar o indivíduo em suas instituições: escolas, hospitais, prisões, etc. No entanto, com todas as mudanças ocorridas até hoje (a segunda Revolução Industrial, as guerras mundiais, a globalização e a internet), Zygmunt Bauman observa que estamos em uma era em que se espera que os indivíduos "se autodisciplinem e arquem com os custos materiais e psíquicos da produção da disciplina", pois as formas de poder não ficam mais atreladas apenas às instituições, mas dependem de uma participação na vigilância de si – o que ele denomina de "sinóptico". Essa participação, pensando na ecologia midiática que nos cerca, é completamente transfigurada em dados e nos rastros que deixamos: as buscas que fazemos, os conteúdos produzidos nas redes e as conversas nas plataformas.

Se essa lógica aparenta um perigo iminente, ela também nos oferta uma grande condição democrática: ao sermos vigilantes de nós, também podemos ser os

***"A ideia de ser vigiado sem perceber foi materializada no final do século XVIII no conceito construído pelo jurista inglês Jeremy Bentham ao criar o panóptico: um projeto de prisão modelada para que todos os prisioneiros sejam observados por alguém sem saberem se estão ou não a serem vigiados"***

vigilantes dos outros e cobrar transparência de qualquer instituição. Diversas associações e empresas se prestam hoje a realizar uma rigorosa análise de dados com as ferramentas Get The Data (fórum que indica como encontrar dados relativos aos mais diversos temas e questões), Is It Open Data? (uma plataforma que ajuda a identificar se determinada base de dados é aberta) e Google Public Data (uma ferramenta que facilita o acesso e a informação de grandes conjuntos em visualizações). Além disso, no caso brasileiro, há também a lei nº 12.527/11, popularmente conhecida como Lei de Acesso à Informação, que assegura a existência e consulta pública de dados públicos para que a sociedade possa tomar conhecimento e investigar. A investigação se tornou o dever cívico dos usuários nas plataformas, pois, em um ambiente de construção de saberes em rede, essa ação coletiva concede inúmeras melhorias nos mais diversos âmbitos econômicos, políticos e sociais.

Esse contexto também possibilita que os usuários recorram a práticas preguiçosas/imediatistas na busca de informações, além de utilizarem as redes para disseminação de notícias e dados falsos com intenções secundárias – uma prática que ajudou a popularizar o conceito de pós-verdade. Iniciativas como a Agência

Lupa, Aos Fatos e Truco baseiam seu modelo de negócios essencialmente nas origens das informações e dos boatos para poderem verificar seu caráter de veracidade. Outros grupos acadêmicos como o Monitor do Debate Político Digital e o Laboratório de Estudos Sobre Imagem e Cibercultura (Labic) têm se utilizado de softwares de coleta de dados em redes sociais com intuito de analisar como se dão as relações entre os usuários e os conteúdos nas redes sociais. Com o auxílio de softwares como o Gelphi e o NodeXL, é possível transformar esses dados em desenhos dinâmicos (grafos) que representam os diferentes níveis de vínculos entre os usuários e os assuntos nas redes em um período de tempo específico.

## Dados disruptivos

Para além da instância crítica do uso de dados, o ambiente convergente das redes também é uma oportunidade grande para a inovação. Desde que as startups se tornaram o modelo de negócio mais dinâmico e de crescimento escalável do mercado digital, diversas ideias nascem ao pensar as tecnologias como ferramentas para solucionar problemas existentes ou que ainda não foram sequer percebidos. Dentro do paradigma do big data, a seletividade dos dados para determinados fins ainda possui vasto campo de exploração. Diversas plataformas têm se especializado em realizar aquilo que o pesquisador francês Fréderic Martel nomeia de *smart curation*, ou seja, processo de curadoria que "se vale ao mesmo tempo da força da internet e dos algoritmos, mas também do tratamento humano e de uma prescrição personalizada feita por curadores".

Plataformas como Netflix e Spotify se tornaram especialistas nessa prática, mapeando os hábitos dos usuários para oferecer a eles os conteúdos mais precisos, de acordo com os hábitos dentro da plataforma. No caso do Netflix, o uso de dados vai além, pois a coleta deles influencia no investimento sobre qual tipo de conteúdo vale a pena ser criado e oferecido para o público, o que transforma todo o formato das narrativas seriadas de acordo com os hábitos dos usuários para os quais eles são endereçados, assim como as decisões de quais atores e diretores deverão ser escalados para a realização do documentário, filme ou série.

Diversas outras iniciativas utilizam os dados e as plataformas para se tornarem intermediárias na hora de entregarem uma solução: empresas como o Planeta Y aproveitam o crescimento do mercado de ensino a distância (EAD) formal e informal, para se especializarem em mineração de dados com o intuito de localizar os usuários com os perfis adequados para um tipo de curso ofertado pelo cliente. A própria atuação com dados também se tornou outro caminho possível como explorado pelo Instituto Brasileiro de Pesquisa de Dados (IBPAD): uma organização que se esforça para disseminar as melhores práticas e também criar cursos para que profissionais das mais diversas áreas possam aprimorar e conhecer o universo complexo das ferramentas e metodologias aplicáveis em âmbito acadêmico e profissional.

> ***"Com a chuva de dados invadindo todas as esferas, o desafio contemporâneo se situa na capacidade de gestão individual e coletiva dessas informações e sua consequente busca de suas prioridades e propósitos"***

## O estado de rede

Essas novas relações surgidas entre os humanos e os objetos abrem possibilidades múltiplas que se alteram constantemente e que nos concedem, pelo menos, uma certeza: já há um gap abissal do século XXI em relação ao já distante século XX. Diferentemente de outros tempos, a nova era exige uma lógica em estado de fluxo permanente, cujo deslocamento e questionamento constantes são mais importantes que a fixação sólida de ideias, padrões e modelos nos mais diversos campos.

Com a chuva de dados invadindo todas as esferas, o desafio contemporâneo se situa na capacidade de gestão individual e coletiva dessas informações e sua consequente busca de prioridades e propósitos. Em meio a um capitalismo cognitivo, cuja produção e circulação de bens imateriais são o grande capital, decidir em quais dados e em quais ações iremos depositar a nossa atenção se tornou a mais valiosa das moedas em nossa economia.

Arquivo pessoal

# A inocência potencializa o risco


**Ivanise Cence**

*Gerente de Segurança da Informação da Prodemge, tem 30 anos de experiência em tecnologia da informação. Graduada em Educação Artística pela Universidade Estadual de Minas Gerais (Uemg). Especializada em Análise de Sistemas pela Prodemge e pós-graduada em Engenharia de Software pela Universidade Federal de Minas Gerais (UFMG), MBA em Gestão Estratégica de Empresas pela Fundação Getúlio Vargas (FGV) e em Gestão de Projetos pelo Instituto de Educação Tecnológica (Ietec). Atuou em suporte, sistemas, produção, banco de dados e negócios.*


O mundo parou no dia 12 de maio de 2017. Quem não se lembra? Naquele dia, todos estavam ligados aos noticiários para saber do que se tratava aquele assunto que ocupou todas as mídias, um ciberataque chamado WannaCry, que ameaçava as pessoas e as empresas. Até um determinado momento, ninguém sabia o que estava acontecendo nem o que fazer. De onde vinha aquela ameaça? Quem poderia contê-la? Pouco a pouco, as respostas foram chegando, o cenário real foi revelado, as correções foram aplicadas. Quem perdeu, perdeu. E a vida continuou como era antes. Ufa! Ainda bem que nada aconteceu comigo, disse Dona Inocência, a secretária executiva. Tão dedicada e eficiente, tinha urgência para saber tudo o que chegava a sua caixa de e-mail. Não deixava nada passar. Abria todas as mensagens e clicava em todos os links, sem distinção. Ela nem imaginava que a própria dedicação tinha colaborado com aquela bomba que descabelava o mundo inteiro. Inocentemente, ela tinha convidado o bandido para jantar.

As organizações investem milhões em inovações tecnológicas aplicadas à segurança cibernética: antivírus, firewall, IDS, IPS, APT, IDM, WAF, criptografia, segregação de redes, gestão de identidade, biometria. Contra as ameaças cibernéticas, aplicam modelos de proteção recomendados pelas melhores práticas.

Mas nada disso consegue conter a Dona Inocência ou aquele jovem destemido e cheio de confiança ou o funcionário teimoso que se vê acima de qualquer regra. Ela continua dedicada e eficiente, e eles, displicentes. Acreditam que estão corretos e não enxergam as consequências. Os cibercriminosos exploram a ingenuidade ou a confiança do usuário para romper barreiras de segurança aparentemente impenetráveis. O elo fraco está sentado na cadeira. Contra ele não há perímetro que

resista. E as ameaças continuam se servindo na mesa dos irresponsáveis e ignorantes.

O anônimo entra anônimo. As ferramentas instaladas no SOC detectam muitos ataques, mas estão sempre em desvantagem em relação aos cibercriminosos. Criativos e velozes, descobrem as vulnerabilidades ainda não reveladas em componentes de hardware e de software e criam novas técnicas e abordagens em uma velocidade proporcional ao volume de soluções e tecnologias ofertadas pelo mercado. Sempre antecipados em relação às empresas, ainda contam com aliados como a Dona Inocência e seus colegas de trabalho.

É possível complementar a eficácia das plataformas instaladas com novas técnicas e tecnologias emergentes. A inteligência analítica é apresentada por especialistas como uma tendência para complementar a eficiência da cibersegurança. É apontada como uma técnica eficaz para detectar uma mudança de comportamento em endpoints e alertar para um possível ciberataque que utilize uma abordagem inédita ou desconhecida. Viabiliza uma resposta rápida ao incidente anunciado de maneira a possibilitar que os técnicos atuem para impedir que o ataque se propague ainda no início da sua jornada.

A segurança cibernética não pode ser vista apenas sob o ponto de vista da tecnologia. O conjunto de recursos tecnológicos e configurações aplicadas para conter as ameaças, por si só, é frágil e incapaz. Ele impede o conhecido, mas não reconhece o inédito. Essa é a maior ameaça. Ela entra invisível através da displicência ou do excesso de confiança do usuário final.

Para potencializar a eficácia da infraestrutura de cibersegurança, é preciso investir também em pessoas e processos, e aspectos como a organização, a conscientização e a responsabilização são essenciais para engajar as pessoas, criar cultura de segurança da informação e mitigar riscos.

## Organização

Não importa muito o tamanho da empresa, o nicho de mercado em que atua ou o seu faturamento. Neste momento de popularização das tecnologias e diversidade de dispositivos ofertados, organizar a segurança da informação é essencial para proteger a informação e garantir e continuidade dos negócios.

É necessário existirem direcionadores objetivos que possibilitem a construção gradual e continuada de uma plataforma consistente e integrada com o uso justo de recursos. Evitar o retrabalho ou o desperdício de tempo e de dinheiro para conter uma ameaça pode ser determinante para a permanência ou a retirada de uma empresa do mercado. É necessário saber como, quando e para onde se pretende ir.

Adotar modelos de gestão e frameworks como guias agiliza os resultados e otimiza os esforços. As normas ISO 27001 e ISO 27002 são referência internacional para a gestão da segurança da informação. Apresentam requisitos para a construção e aplicação de um Sistema de Gestão da Segurança da Informação (SGSI) por meio de uma abordagem de gestão de risco no negócio.

Em termos práticos, o SGSI é um conjunto documentado de direcionadores construídos a partir da realidade da empresa e com a finalidade de indicar projetos para proteger a efetiva proteção das informações de acordo com os princípios da segurança da informação e o cenário das ameaças.

Conhecer o nível de maturidade em que se encontra a empresa é fundamental. Uma análise de riscos do negócio viabiliza elaborar de forma objetiva e fundamentada um plano de segurança da informação com estratégias, direcionadores e a indicação de ações práticas voltadas para a tecnologia, os processos e as pessoas. Ciclos PDCA devem ser realizados periodicamente para garantir o alinhamento dos direcionadores com a realidade da empresa, com as tendências em segurança da informação.

Elaborar uma arquitetura de referência com a projeção da plataforma de cibersegurança que se pretende construir é outra providência que não pode ser desconsiderada. Ela será utilizada para dimensionar e organizar os dispositivos tecnológicos e definir projetos tecnológicos integrados e complementares. O NIST (Cybersecurity Framework) pode auxiliar na organização de uma plataforma mais segura.

Ter clareza sobre as responsabilidades em segurança da informação é condicionante para evitar a sobreposição de funções ou o descuido com pontos fundamentais. Uma mudança na estrutura organizacional pode ser necessária para adaptar a empresa às necessidades da segurança.

Priorizar as políticas, normativos e procedimentos necessários para direcionar as pessoas também é um condicionante para a organização.

Um patrocinador forte que compreenda o real valor da segurança da informação para os negócios e fomente os projetos, investimentos e ações facilita o processo de organização e o seu resultado.

## Conscientização

O entendimento das pessoas sobre segurança da informação é tão importante quanto a segurança cibernética implementada nas plataformas de TIC. Michael Santarcangelo[1] definiu "conscientização para a segurança" como "a percepção individual das consequências de uma ação, aliada à habilidade de avaliar sua intenção e seu impacto".

Criar documentos de segurança e torná-los públicos não é suficiente para que as ações e os direcionadores gerados na organização para a segurança sejam conhecidos e seguidos pelas pessoas.

Os autores da publicação *Building an Information Technology Security Awareness and Training Program* do NIST dizem: "A razão da conscientização é focar atenção na segurança. Deve ajudar os indivíduos a reconhecer as preocupações da área de segurança da informação e responder corretamente". Cada novo direcionador criado deve ser efetivamente apresentado a cada um dos integrantes da empresa. A equipe da segurança deve ser insistente e, se for necessário, repetitiva de maneira que os temas e assuntos se tornem parte da rotina. As pessoas precisam se preocupar com a segurança que deve ser naturalmente considerada nos processos.

Um plano formal de treinamento em segurança da informação para os empregados é um grande facilitador na disseminação e formação de conhecimento e na construção de uma cultura forte em segurança.

Campanhas de sensibilização são recomendadas pelas melhores práticas como um recurso fundamental para a disseminação da segurança. Podem ser utilizadas para apresentar as técnicas da engenharia social adotadas para enganar os distraídos e inocentes. Ao explicar as formas que os cibercriminosos utilizam para invadir os ambientes, os profissionais de TIC são incentivados a construir sistemas mais seguros.

Conscientização para a segurança é um ciclo que deve ocorrer de forma continuada e alcançar indistintamente todos que participam dos processos: empresa, colaboradores e fornecedores. Dos que ocupam as funções mais estratégicas àqueles que executam atividades operacionais.

## Responsabilização

A exposição indevida de informações ou o acesso desautorizado a uma informação representam um risco que interfere negativamente nos negócios. Desfazer o comprometimento da imagem de uma empresa associada a um ato de violação dos princípios da confidencialidade ou da integridade tem custo alto. Dependendo do tamanho, o dano é irreparável e o esforço é pouco útil. Prevenir é mais barato do que combater.

> ***"É preciso repensar a segurança e rever a forma como ela é tratada. Investir nas plataformas digitais é fundamental, mas frente à diversidade de técnicas de invasão, todos os colaboradores precisam estar cientes do seu papel na segurança da informação"***

Os indivíduos muitas vezes se desconectam das consequências dos seus atos. De forma inocente ou intencional, desprezam os riscos que podem comprometer a empresa ou a sua vida privada.

A assinatura de termos de responsabilidades e a inclusão de cláusulas de segurança em contratos formalizam regras e viabilizam compartilhar responsabilidades entre a empresa e seus colaboradores. É preciso tornar todo funcionário responsável pelos dados que passam por ele e apresentá-lo aos riscos potenciais de seus atos.

É preciso repensar a segurança e rever a forma como ela é tratada. Investir nas plataformas digitais é fundamental, mas, frente à diversidade de técnicas de invasão, todos os colaboradores precisam estar cientes do seu papel na segurança da informação. Ações voltadas para as pessoas constituem a base para a construção de uma cultura forte em segurança. Com o empenho e a conscientização das pessoas em segurança da informação, será necessário investir menos em tecnologia, e a inocência poderá ser vista como uma virtude.

1 Disponível em https://securitycatalyst.com/why-the-definition-of-security-awareness-matters/

Arquivo pessoal


**Leonardo Barbosa e Oliveira**

*Professor do Programa de Pós-Graduação em Ciência da Computação da Universidade Federal de Minas Gerais (UFMG), professor associado visitante da Universidade de Stanford e bolsista de Produtividade em Pesquisa do Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq). É membro do Comitê Consultivo da Comissão Especial de Segurança da Informação e Sistemas Computacionais da Sociedade Brasileira de Computação, membro do Comitê de Gestão de Identidade da Rede Nacional de Ensino e Pesquisa e coordenador do Grupo de Pesquisa Segurança Digital, Criptografia e Privacidade do CNPq.*


# O computador para o século XXI: desafios de segurança e privacidade após 25 anos[1]

Em 1991, Mark Weiser descreveu uma visão do computador para o século XXI [Weiser 1991]. Weiser, em seu artigo profético, argumentou que as tecnologias mais abrangentes são as que se tornam transparentes. De acordo com ele, esse esquecimento é um fenômeno humano – não tecnológico: "Sempre que as pessoas aprendem algo suficientemente bem, elas deixam de estar cientes disso", afirmou. Esse evento é chamado dimensão tácita ou compilação e pode ser testemunhado, por exemplo, quando os motoristas reagem aos sinais de rua sem, conscientemente, ter que processar as letras P-A-R-E.

Um quarto de século depois, no entanto, o sonho de Weiser está longe de se tornar realidade. Ao longo dos anos, muitos dos conceitos dele sobre computação ubíqua (Ubiquitous Computing – UbiComp) foram materializados no que hoje chamamos de redes de sensores sem fio (Wireless Sensor Networks – WSNs), internet das coisas (Internet of Things – IoT), computação vestível (Wearable Computing) e sistemas-ciber-físicos (Cyber-Physical Systems – CPSs).

As aplicações desses sistemas abordam desde a prevenção de acidentes de trânsito, passando pelo monitoramento de emissões de $CO_2$ no contexto de carros autônomos até o tratamento de pacientes domésticos. Por outro lado, apesar de todos esses benefícios, o advento desses sistemas trouxe consigo, também, problemas de segurança. E, a menos que os abordemos adequadamente, o futuro da profecia de Weiser estará em jogo.

A UbiComp nos desafia com novos problemas de segurança porque exibe uma perspectiva totalmente diferente da computação tradicional. Nela, os elementos

1 Este texto é parte de um trabalho já publicado [Oliveira *et al.* 2017] dos autores Leonardo B. Oliveira, Fernando M. Q. Pereira, Rafael Misoczki, Diego F. Aranha, Fabio Borges e Jie Liu.

computacionais apresentam sensores, CPU e atuadores, o que significa que eles conseguem, respectivamente, ouvir (ou espionar) você, processar seus dados (e, possivelmente, descobrir algo sigiloso sobre você) e responder às suas ações (ou, em última análise, revelar algum segredo). Tais capacidades, por sua vez, tornam as propostas para computadores convencionais inadequadas no contexto de UbiComp e, por fim, colocam-nos diante de novos desafios.

Muitos deles estão nas áreas de segurança e privacidade, embora, contraditoriamente, à medida que elementos computacionais permeiam nossas vidas, a demanda por esquemas de segurança mais fortes se torna ainda maior. Particularmente, existe uma necessidade extrema de um mecanismo de segurança capaz de abarcar todos os aspectos e manifestações de UbiComp, tanto no tempo como no espaço, e de maneira perfeita e eficiente.

A seguir, apresentamos alguns tópicos de segurança e privacidade no contexto de UbiComp que nos desafiam, atualmente:

1) Proteção de software. A adoção de linguagens com tipos fracos (weakly typed languages) bem como software poliglotas (escritos em diferentes linguagens de programação) por dispositivos com recursos limitados pode levar a sistemas vulneráveis. É necessário conceber técnicas exclusivamente propostas para analisar esses tipos de sistemas.

2) Segurança em longo prazo. É essencial revisitarmos a segurança de criptossistemas amplamente utilizados (por exemplo, RSA/ECC), divulgando ameaças trazidas à tona recentemente (com os avanços em criptoanálise e ataques quânticos) e norteando os caminhos para que se garanta segurança de longo prazo no contexto de UbiComp.

3) Engenharia de criptografia. É preciso reafirmar o papel essencial da criptografia na proteção de computadores, discutindo o estado atual dos criptossistemas leves, sua implementação segura e como os mesmos interagem com os protocolos de gerenciamento de chaves criptográficas.

4) Implicações na privacidade. A segurança é necessária, mas não suficiente para garantir a privacidade, como identificação e regulação de dados sensíveis frente a novos métodos de defesa (protocolos de preservação de privacidade baseados em criptografia homomórfica).

Acreditamos que, se compreendermos tanto os desafios como os novos rumos corretamente, conseguiremos então transformar a ficção científica da UbiComp em ciência de fato.

## Referências


ABOWD, G. D. and MYNATT, E. D. (2000). **Charting past, present, and future research in ubiquitous computing**. ACM Transactions on Computer-Human Interaction, 7(1):29–58.

ASHTON, K. (2009). **That 'Internet of Things' Thing**. RFiDJournal. 22:97–114.

ATZORI, L.; IERA, A. and MORABITO, G. (2010). **The Internet of Things: A survey**. Computer Networks, 54(15):2787–2805.

ESTRIN, D.; GOVINDAN, R.; HEIDEMANN, J. S. and KUMAR, S. (1999). **Next century challenges: Scalable coordination in sensor networks**. In MobiCom'99, p. 263–270.

LEE, E. A. (2006). **Cyber-physical systems-are computing foundations adequate.** In NSF Workshop on Cyber-Physical Systems: Research Motivation, Techniques and Roadmap, v.2. Citeseer.

LYYTINEN, K. and YOO, Y. (2002). **Ubiquitous computing.** Communications of the ACM, 45(12):63–96.

MANN, S. (1997). **Wearable computing: A first step toward personal imaging**. Computer, 30(2):25–32.

MARTIN, T. and HEALEY, J. (2007). **2006's wearable computing advances and fashions**. IEEE Pervasive Computing, 6(1).

OLIVEIRA, L. B.; ao PEREIRA, F. M. Q.; MISOCZKI, R.; ARANHA, D. F.; BORGES, F. and LIU, J. (2017). **The computer for the 21st century: Security & privacy challenges after 25 years**. In 2017 26th International Conference on Computer Communication and Networks (ICCCN).

POTTIE, G. J. and KAISER, W. J. (2000). **Wireless Integrated Network Sensors**. Communications ACM, 43(5):51–58.

RAJKUMAR, R. R.; LEE, I.; SHA, L. and STANKOVIC, J. (2010). **Cyber-physical systems: the next computing revolution**. In 47th Design Automation Conference. ACM.

SOUZA, A.; CUNHA, Í. and B OLIVEIRA, L. (2017). **NomadiKey: User Authentication for Smart Devices based on Nomadic Keys**. International Journal of Network Management, p. e1998–n/a.

STAJANO, F. (2002). **Security for Ubiquitous Computing**. John Wiley and Sons.

WEISER, M. (1991). **The computer for the 21st century**. Scientificamerican, 265(3):94–104.

WEISER, M. (1993). **Some computer science issues in ubiquitous computing.** Communications of the ACM, 36(7):75–84.

Arquivo Pessoal


## Marcos Calmon

*Presidente da Safe Security Solutions Ltda., empresa com mais de 15 anos de atuação no mercado de construção de data centers, e do Centro Integrado de Comando e Controle (CICC), além de produtos e serviços de segurança da informação e infraestrutura de tecnologia da informação. Conselheiro da Câmara Internacional de Negócios (CIN), câmara de comércio internacional bilateral em que funcionam as câmaras de comércio Brasil-China, Brasil-Guatemala, Brasil-Canadá, Brasil-Rússia, Brasil-Moçambique e Brasil-Austrália. Possui mais de 20 anos na área de Tecnologia da Informação e Comunicação (TIC), dos quais mais de 15 anos como especialista em segurança da informação.*


# O seu mundo vai virar de cabeça pra baixo! E como fica a segurança da informação nisso tudo?

A 4ª Revolução industrial já está acontecendo. Você está preparado para vivenciar essa transformação digital que interliga sistemas digitais, físicos e biológicos? Estamos vivendo uma era de transformação na qual a tecnologia é o personagem principal e modifica todos os modelos de negócios e relações pessoais que adquirimos até hoje. Mas, antes de explicar sobre a 4ª Revolução Industrial, vamos lembrar as três revoluções anteriores que marcaram a nossa história.

A 1ª Revolução aconteceu em meados do século 18 e foi marcada pela invenção da máquina a vapor e a aplicação dela na fabricação de produtos têxtis, trazendo muitas modificações na economia e na sociedade com a geração de mais empregos, a expansão de fábricas, o aumento de imigrantes e, consequentemente, o aumento das cidades onde se concentravam as produções.

Era preciso agilizar o fornecimento de matéria-prima e muitos meios de transporte foram construídos e aprimorados. Depois desse grande salto na nossa economia, vivenciamos a 2ª Revolução Industrial durante a segunda metade do século XIX e que terminou durante a 2ª Guerra Mundial. O principal motivo foi o desenvolvimento de indústrias elétricas, químicas, de petróleo, aço e a produção em massa de bens de consumo. Após a 2ª Guerra Mundial, diversas evoluções aconteceram no campo tecnológico, principalmente para automatizar os processos de produção industrial em massa. Foi um período de muitas pesquisas e descobertas que permitiram o desenvolvimento industrial por meio de tecnologias.

Além de informatizar os processos, a robótica, os chips, a produção de computadores, telefones móveis e softwares trouxe uma nova perspectiva para os negócios, resul-

tando em maior produtividade e oportunidades de expansão dos mercados. Por fim, vamos falar sobre a 4ª Revolução Industrial que se iniciou na virada do século XXI e promete ficar.

Impulsionada pela sinergia entre inteligência artificial, robótica, nanotecnologia, impressões 3D, internet das coisas, mundo físico e biológico, a 4ª Revolução mostra um novo cenário no qual temos (e teremos ainda mais) uma cadeia produtiva extremamente conectada e processos adaptáveis a qualquer situação e necessidade. Uma coisa é certa: seu mundo vai virar de cabeça pra baixo! Já conseguimos vivenciar essa revolução quando acessamos nossos smartphones e solicitamos transporte via Uber – empresa que não possui automóveis e os motoristas credenciados trabalham a favor dela. Vemos essa mesma situação quando estamos planejando uma viagem e reservamos uma casa pelo Airbnb, o maior provedor de hospedagem do mundo, que também não possui nenhuma propriedade.

Com essas modificações no cenário mercadológico, existem hoje inúmeras possibilidades de trabalhos virtuais e as relações de trabalho pessoais estão ficando mais escassas. Os computadores e as grandes empresas virtuais, estão tomando cada vez mais o lugar de humanos. Como ponto positivo para o desenvolvimento, a tecnologia da informação traz significativa redução de custos nos processos, agrega velocidade e diminui erros e desperdícios, otimiza recursos em tempo recorde e aumenta ainda mais as chances de lucros e novos negócios para as organizações.

Mas, afinal, como seu mundo vai virar de ponta-cabeça? Vale aqui uma reflexão: Como será nossa educação se cada vez mais temos faculdades e escolas de ensino a distância? Como serão as relações sociais, sendo que grupos virtuais e comunidades se formam a cada segundo? Como será nosso futuro, visto que as máquinas estão tomando nossos empregos?

Está fritando a massa encefálica?

As tecnologias deverão chegar para melhorar e não dominar os nossos espaços. É preciso reinventar as formas de trabalho e se adequar ao novo.

As informações chegam extremamente rápido. Em segundos, temos uma novidade acerca de um fato ocorrido em qualquer parte do mundo. A questão e o segredo é utilizar essas informações a nosso favor – além de aprender com as inovações, é preciso acompanhar e crescer. Hoje, as informações valem mais do que qualquer dinheiro. A revolução tecnológica nos traz outro termo que hoje está sendo muito utilizado e estudado: IoT - Internet of Things ou internet das coisas, em nossa língua.

IoT possui várias possibilidades de transformar as nossas relações com a tecnologia e modifica a maneira como lidamos com o mundo e como o mundo lida conosco. De modo geral, é a maneira como as coisas estão conectadas e como se comunicam com o usuário por meio de sensores inteligentes e softwares bem estruturados, que transmitem dados para uma rede global, onde todas as suas informações estão conectadas. Como exemplo, citamos um carro que possui um aplicativo instalado no smartphone do seu dono, que lhe avisa, com mensagens de texto ou voz, se o pneu precisa ser calibrado, se o óleo precisa ser trocado ou até mesmo para avisar que a rota que você está habituado a fazer naquela manhã está congestionada, portanto, melhor ir por outra, já sugerida por ele, o aplicativo. Todas as ações se tornam responsivas e inteligentes e, por isso, é possível identificar grandes falhas e prevenir possíveis problemas. Internet of things é um exemplo claro da 4ª Revolução Industrial, na qual interligamos tecnologia, física e biologia de maneira inteligente.

Com a 4ª Revolução Industrial, ou transformação digital, como prefiro chamar, iremos confundir o natural com o artificial. No campo físico, iremos confundir o que foi criado pelo homem com o que foi criado por Deus, com a já real capacidade de visualizar as nossas atividades cerebrais por meio de dispositivos EEG – Eletroencefalográficos, abrindo a "caixa preta" do cérebro e nos permitindo entender coisas nunca antes vistas sobre a nossa relação com a vida, com o planeta, com as pessoas, com o trabalho, etc. Uma vez isso mapeado e entendido, podemos criar um planeta muito mais harmônico, eficiente e personalizado. Poderemos, por exemplo, fazer paralíticos andarem novamente ou curar dependentes químicos.

Imagine não precisar mais dos plásticos para fazer materiais, mas transformar funcionalidades biológicas para obter materiais não nocivos ao planeta e com as mesmas funcionalidades das de plástico. Imagine utilizar tecnologias energéticas, como solar, eólica ou biomassa, para criar uma grande rede de energia em que haja integração de toda a rede de um continente, utilizando o vento que passa no Chile e o sol do Nordeste do Brasil para passar e distribuir, por meio de uma grande rede interconectada, energia a todos que dela precisam e a qualquer momento.

Diante desse cenário cada vez mais conectado, devemos nos questionar como fica a segurança de nossas informações, visto que estamos cada vez mais expostos e nossos dados estão registrados em uma rede mundial. Como podemos nos proteger diante disso? Quais medidas devemos tomar para que os dados de nossas empresas e nossos dados pessoais não corram riscos nessa grande rede?

A internet das coisas causará impacto muito grande nas relações humanas e nos negócios; o perfil de compra do consumidor e os hábitos de consumo serão modificados. Na visão do empresário, é necessário interpretar todos os dados coletados na grande rede global para entender as necessidades do novo mercado e oferecer, mais que os produtos necessários, uma boa experiência de compra.

A compra de dispositivos inteligentes está cada vez maior. De acordo com o relatório de ameaças à segurança da internet realizado pela Symantec em abril de 2017, existe mais de um smartphone por pessoa no mundo. Estamos falando de bilhões de aparelhos que se conectam, aparelhos de última geração, de alta qualidade, com poderosos processadores e boas conectividades. Esses smartphones guardam informações valiosas, como senhas e acessos restritos, o que pode trazer alta vulnerabilidade para o usuário em caso de perda ou sabotagem dos dados.

Ataques DDoS, fishing, ransomwares e spam têm se tornado os tipos mais comuns e muito atraentes por três razões:

**1)** A segurança da informação não é primordial para o fabricante do dispositivo, sendo assim as senhas são padronizadas, muitas portas são abertas e, em diversos casos, senhas não podem ser trocadas.

**2)** As atualizações do firmware, em muitos casos, não são automáticas, o que torna o dispositivo mais vulnerável.

**3)** Uma vez instalado, o firmware e demais aplicativos são esquecidos. Sendo assim, o usuário não sabe para quais fins seus dados estão sendo utilizados.

Os dispositivos IoT, quando infectados, podem ser usados como um passo para atacar outros dispositivos em uma rede privada e acontecer o que chamamos de botnet (rede de robôs) global, que é quando o seu dispositivo recebe um malware e é transformado em um bot (robô), no qual o dispositivo executa tarefas mal-intencionadas sem que você saiba, tudo isso em grande escala.

A primeira ação a ser tomada para evitar ataques é trocar as senhas dos dispositivos. De acordo com o relatório da Symantec, os nomes de usuários, na maioria dos casos, não mudam, e as senhas mais utilizadas são: abc123, admin123, test, 1234, password, ubnt, 12345, 123456, root e admin.

Muitos usuários provavelmente não sabem do perigo que correm ao deixarem credenciais padrão e não alterarem nomes de usuários já cadastrados de fábrica.

Em 2016, incríveis 18,4 milhões de dispositivos foram atacados por malwares! Algumas boas práticas deverão ser adotadas para evitar ao máximo a exposição de seus dados e vulnerabilidades na rede, como:

- Pesquise qual o nível de segurança no dispositivo, antes de comprá-lo;
- Faça uma análise dos dispositivos conectados em sua rede privada;
- Altere as senhas, utilize combinações fortes com caracteres especiais, números e letras maiúsculas e minúsculas para dispositivos e wi-fi;
- Configure a rede wi-fi com criptografia forte e senha segura;
- Quando for hospedar suas informações em nuvem (cloud, no inglês), escolha locais seguros, de empresas confiáveis;
- Muitos dispositivos vêm com serviços diversos habilitados por padrão de fábrica, desabilite-os caso não sejam utilizados;
- Modifique as configurações de privacidade e segurança padrão dos dispositivos de acordo com a sua necessidade;
- Verifique sempre no site do fabricante as informações sobre atualizações de firmware e habilite essas atualizações para automáticas, sempre que possível.

Executando essas ações, você não estará totalmente protegido, mas deixará o caminho mais longo para as ameaças da internet. E lembre-se: uma pessoa prevenida vale por duas!

Arquivo pessoal

# Blockchain e a autenticidade de informações para a democracia


## Marco Konopacki

*Doutorando em Ciência Política pela Universidade Federal de Minas Gerais (UFMG), graduado em Administração e mestre em Ciência Política pela Universidade Federal do Paraná (UFPR). Foi professor visitante do Instituto Tecnológico da Aeronáutica (ITA) nas áreas de gestão de desenvolvimento de software, telemetria e georreferenciamento. É gestor e pesquisador de temas relativos à Governança de Tecnologia da Informação, Desenvolvimento de Software, Participação Social e Participação Política, com vasto histórico de atuação nos setores público e privado. Foi assessor da Secretaria de Assuntos Legislativos do Ministério da Justiça, onde coordenou o debate público para regulamentação do Marco Civil da Internet. Atualmente, é coordenador de projetos na linha de democracia e tecnologia do Instituto de Tecnologia e Sociedade (ITS) Rio.*


A tecnologia ainda é usada de maneira tímida em processos para ampliação da participação efetiva de cidadãos. Quando falamos da presença de milhões de pessoas envolvidas em discussões políticas de assuntos de seus países, precisamos pensar em modelos mais robustos e sofisticados para acolher as diferentes opiniões. Hoje, apesar de todos os avanços e da popularização das tecnologias de informação e comunicação (TIC), a tecnologia ainda ocupa um posto dispensável na forma como a política é pensada, operada e organizada. Por isso, é interessante observar como alguns algoritmos operam rotinas de decisão em grande escala e como isso poderia inspirar a construção de normas a partir de consensos com o apoio da tecnologia. O melhor caso para ilustrar esse cenário são as redes abertas de dados distribuídos baseadas em blockchain.

Blockchain é a rede de computadores responsável por fornecer um banco de dados descentralizado utilizado para viabilizar transações entre nós de sua rede, permitindo a existência do bitcoin, moeda virtual criada em 2007, que opera 100% de suas operações financeiras no formato digital, fazendo com que hoje seja a aplicação mais popular e valiosa da rede. A blockchain, ou cadeia de blocos, se fundamenta em técnicas de criptografia e computação distribuída para criar uma rede de transações de dados autenticadas e sem intermediários. A rede não se resume apenas ao bitcoin, existe uma infinidade de outras aplicações possíveis que vêm sendo construídas tirando proveito da arquitetura descentralizada.

O ponto crucial da blockchain é o consenso. Por se tratar de um banco de dados distribuído e aberto, significa que diferentes computadores possuem uma cópia do banco de dados e a cada minuto novos computadores podem se juntar à rede sem nenhuma autorização prévia, desde

que concordem com três princípios: 1) adotem o mesmo conjunto de dados; 2) a forma como esses dados são modificados; e 3) as regras que regem o armazenamento e o processamento de dados.

Para gerenciar e garantir a harmonia, as redes blockchain possuem algoritmos para organizar regras automáticas para obtenção de consenso. Essas regras gerenciam se o conjunto de dados compartilhados é válido, ou seja, verifica se nenhum nó da rede tentou fraudar uma transação. Cada transação na blockchain é assinada digitalmente. Esses algoritmos conseguem verificar as assinaturas sem revelar nenhuma informação do emissor da mensagem, da mesma forma que regras automáticas estabelecem qual o formato da mensagem para geração de novas transações e como elas podem ser validadas. Essas regras são públicas, de código aberto e disponíveis para verificação por qualquer nó da rede.

Regras de autorregulamentação para gerenciar redes distribuídas não são novidade. Elas fazem parte da própria origem da internet com a criação dos primeiros protocolos. O que a blockchain oferece como inovação é a possibilidade de desfrutar de algoritmos com regras transparentes que democratizam as tomadas de decisões complexas sobre a operação e gestão de dados.

Por ser uma rede distribuída, é necessário estabelecer uma regra pública para decidir quem escreve no banco de dados. A rede do bitcoin elegeu uma regra que evitasse a concentração de poder na rede e seu algoritmo concede direito de escrita àqueles nós da rede que resolvam um desafio matemático, uma espécie de Sudoku complexo. O primeiro a encontrar a solução do desafio é recompensado com uma quantia em moedas virtuais, ou seja, existe uma retribuição monetária direta em bitcoins ao mesmo tempo em que há um esforço para aumentar o poder de processamento da rede. Isso cria um estímulo para os diferentes nós protegerem o bom funcionamento do conjunto de dados, ao invés de atacá-lo para tentar obter alguma vantagem exclusiva.

Da mesma forma que numa democracia, na blockchain existem regras que tornam o processo de validação e decisão transparente. É em torno dos consensos dos procedimentos que a rede estabelece a confiança entre os diferentes nós. Quando é necessária a tomada de decisão, um algoritmo público (que seria análogo a regras públicas e transparentes sobre como representantes são eleitos, por exemplo) arquiteta a decisão e informa a rede. Se por acaso um nó eleito para produzir um novo bloco agir de má fé, é possível que ele ponha em risco a confiança de outros nós, o que o levaria também ao seu próprio prejuízo, uma vez que esses nós têm algum tipo de motivação para o fortalecimento da rede.

O modelo de consenso automatizado da blockchain é um caso interessante a ser estudado. É intrigante imaginar que a conjugação de esforços para produzir bens comuns à rede tenha funcionado tão bem para o modelo do bitcoin. Nessa rede, o incentivo para que ela se fortaleça e seja protegida pelos diferentes nós está na proteção do valor econômico que a rede adquiriu com o passar do tempo. Será que esse modelo teria êxito para construção de leis? Existem incentivos, fora os financeiros, que possam unir e fazer com que diferentes atores alinhem-se com o propósito de proteger e promover uma rede auto-organizada interessada em construir novas leis?

Com a aprovação do fundo bilionário para financiamento de campanhas, muito tem se falado sobre os custos para suportar a democracia. Não se pode querer imaginar o modelo da república de Platão aplicada aos dias de hoje, em que os políticos são seres sem preocupações pessoais e dedicados exclusivamente a tudo aquilo considerado público. Lembremos que, na época de Platão, a pólis era gerida pelos nobres gregos, os únicos realmente considerados cidadãos, excluindo-se diferentes classes daquele sistema. Ou seja, não havia preocupações econômicas por aqueles que geriam a política.

A democracia moderna são sistemas complexos. A universalidade do acesso ao sistema político deve compreender que os agentes políticos possuem diferentes origens de vida e essa origem não pode determinar o sucesso ou não daqueles que participam desse sistema. Ao contrário, ele deve estimular a busca pela igualdade de condições entre aqueles que participam. Para isso, é necessário construir mecanismos de incentivo e financiamento desse sistema que estejam disponíveis para todos, com regras públicas e transparentes para acesso a esses recursos.

Blockchain é uma tecnologia que pode transformar esse cenário e dar segurança para informação que legitima a atuação dos atores no sistema político. Imagine um cenário em que existam regras transparentes em que quanto mais um agente contribuir para a democracia, mais recurso ele poderá obter para investir na sua campanha política. Isso poderia ser autenticado por uma rede distribuída que daria validade a essas ações, evitando as fraudes e distorções que percebemos hoje nas regras do jogo democrático. Essas possibilidades já estão disponíveis e graças à inventividade de empreendedores sociais e políticos, quando essas tecnologias passarem a se tornar populares, experimentaremos novos patamares na melhoria de nossas democracias.

Arquivo pessoal

# IoT (Internet of Things): um desafio para a cibersecurity


**Paulo Furiati**

*Graduado em Processamento de Dados pela Fabrai e pós-graduado em Segurança da Informação pela Universidade Fumec. Mestrando em Tecnologia da Informação Aplicada pelo Promove. Profissional atuando na área de segurança da informação desde 2003. Já atuou em empresas de diversos segmentos, como financeiro, cartões de crédito e governo. Atualmente, é professor universitário na área de SI e atua na área de governo.*


Segundo projeções, estima-se que, em 2020, teremos mais de 20,4 bilhões de dispositivos conectados. Um crescimento expressivo se levarmos em conta que a estimativa para 2017 é de 8,4 bilhões de dispositivos conectados, ultrapassando, assim, a barreira de um dispositivo por habitante.

O espectro de abrangência da aplicação desses dispositivos permeia praticamente todas as áreas em que a tecnologia pode ser utilizada, desde o uso na automação residencial até o industrial, perpassando pelas áreas de saúde, financeira, automobilística, educacional, dentre outras.

Diante de números tão expressivos, praticamente todos os grandes fabricantes de tecnologia estão trabalhando com foco nessa plataforma (de maneira direta ou indireta), o que torna ainda mais relevante a preocupação com segurança, seja por parte do usuário doméstico, seja para uso comercial e/ou industrial.

Em contrapartida, até julho deste ano, já foram identificadas pelo menos 7.000 vulnerabilidades presentes em dispositivos IoT, mais que o dobro que as encontradas em todo o ano de 2016. No Brasil, um em cada cinco dispositivos é vulnerável. Webcans, impressoras, roteadores, babás eletrônicas estão no rol de equipamentos vulneráveis. A cada dia que se passa, é mais comum aparecerem na internet relatos de equipamentos invadidos e/ou comprometidos em que a privacidade dos usuários foi violada ou o atacante conseguiu acesso e controle desses dispositivos sem autorização. Para exemplificar esse fato, em 2013, um atacante obteve acesso a uma babá eletrônica na cidade de Hebron, Ohio, nos Estados Unidos, onde ele, durante a noite, gritava: "Acorda neném", deixando os pais do bebê de 10 meses apavorados. Quando chegaram ao quarto da criança, presenciaram a câme-

ra da babá eletrônica se movendo, apontando em direção ao pai e falando diversos impropérios. A reação imediata do pai foi desligar o equipamento. Esse caso é apenas a ponta do iceberg, um dos pontos a serem considerados.

Já no campo corporativo, existem grandes preocupações com a utilização de dispositivos IoT para a composição de botnets, redes zumbis capazes de realizar ataques coordenados de acordo com o comando dos seus gerenciadores. Em setembro de 2016, a botnet Mirai, que é composta, em sua essência, por dispositivos IoT contaminados, na sua primeira aparição, deixou aproximadamente 1 milhão de alemães sem internet por um final de semana. Para se ter ideia da capacidade destrutiva dessa botnet, em um de seus ataques (DDoS), estima-se que foram utilizados 100 mil dispositivos infectados, gerando um tráfego de extraordinários 1,2Tbps.

Esses são apenas exemplos, mas não são casos isolados e não se limitam a esse tipo de interferência externa em sistemas IoT. Temos aqui a dimensão do problema a que podemos estar sujeitos, caso a segurança dos sistemas seja negligenciada.

Se levarmos em conta que o ecossistema de IoT compreende sensores, dispositivos e equipamentos conectados que podem transmitir e receber informações com o objetivo de rastreamento, análise e/ou monitoramento e, em vários casos, acionamentos diversos, podemos ter uma ideia do quão complexo é o processo de segurança envolvido. Assim sendo, a segurança deve ser uma preocupação em todas as etapas do processo de desenvolvimento e uso desses dispositivos.

Sob o ponto de vista da segurança da informação, apesar de o objetivo final ser a minimização dos riscos com o uso da tecnologia e o pensamento ser concentrado na proteção de todo o sistema, podemos usar conceitos de proteção conhecidos para cada um dos seis componentes individualmente, abordando seus processos, peculiaridades e também vulnerabilidades.

Abordemos então os pontos-chave de cada um dos componentes dos sistemas IoT:

**USER:** podemos dividir esse componente em pelo menos três grandes grupos: usuários domésticos, usuários corporativos e outros devices (M2M – Machine to Machine). Vamos concentrar nossos esforços nos dois primeiros, uma vez que, em momento adequado, voltaremos a falar especificamente da segurança dos dispositivos.

Nos dias atuais, a maioria das corporações já tem seus processos relacionados à segurança na utilização de dispositivos diversos e trata o assunto com prioridade (se não trata, deveria tratar!). Existem as políticas de segurança e demais processos e procedimentos que abordam o assunto. A utilização de IoT passa, assim, a ocupar mais um item em todo esse processo. E, sim, deve receber atenção especial! As tecnologias são novas e trazem grandes desafios para os administradores de TI do ambiente, seja possibilitando que cibercriminosos se apoderem dos equipamentos para serem participantes de uma botnet, seja para realizar ataques laterais dentro da própria rede corporativa. As possibilidades são muitas e os objetivos de possíveis abordagens também.

Quanto aos usuários domésticos, na maioria dos casos, são duas as preocupações básicas (mas não se limitando a elas):

**1)** Preservação de privacidade (obtenção de informações pessoais por meio da rede, como cartões de crédito, dados bancários, etc., até a exposição de imagens privadas na internet).

**2)** Evitar que seus equipamentos sejam utilizados para ataques a outros dispositivos (dispositivo zumbi).

Parece impressionante, mas a mesma pesquisa que identificou que 1/5 dos dispositivos no Brasil é vulnerável identificou também que uma das brechas de segurança mais encontradas foi a utilização de credencial padrão do fabricante (usuário e senha), que permitia acesso total aos dispositivos como roteadores, câmeras ip, babá eletrônica, dentre outros. As recomendações de proteção nesse caso passam por medidas simples e que são amplamente divulgadas, como por exemplo: mudar a senha padrão dos dispositivos, mas notoriamente não seguida pelos usuários. Cabe aqui uma reflexão. Para um usuário leigo, não é fácil se familiarizar com toda essa inundação de informações, o que não o exime da responsabilidade de usar a tecnologia com segurança. Por outro lado, acredito que os fabricantes podem (e devem) desenvolver produtos não somente amigáveis (ligou, funcionou!), mas que eles sejam também seguros.

**DEVICES:** Para direcionar os fabricantes e qualquer um que queira desenvolver dispositivos IoT, uma vez que facilmente encontramos soluções baseadas em DIY (Do It Yourself – faça você mesmo) utilizando plataformas como o Arduino[1], já estão em fase de desenvolvimento normas para padronização e segurança no desenvolvimento de dispositivos. As normas ISO 20924 e 30141 serão as responsáveis pelo tratamento do assunto. Além disso, alguns fabricantes têm aplicado conceitos mais sofisticados para manter a segurança dos equipamentos, dentre eles, podemos citar:

- Chip security, na forma de TPM (Trusted Plataform Modules), em que informações sensíveis têm acesso restrito a credenciais específicas e chaves de criptografia são armazenadas internamente no chip.
- Boot seguro, prevenindo que software não verificado seja executado no equipamento.

Com relação ao software embarcado no device, a recomendação também não difere do desenvolvimento seguro de qualquer outra solução de software, seguindo os códigos de boas práticas e outros procedimentos amplamente adotados pelo mercado.

Todos os pontos mencionados valem também quando se utiliza o dispositivo como "cliente" (M2M), garantindo a proteção necessária a todo o sistema.

**GATEWAY, CONEXÃO, CLOUD:** A essência do sucesso da tecnologia IoT está baseada justamente na capacidade de comunicação, na troca de informações, no armazenamento e na disponibilidade de dados dos dispositivos. A infraestrutura então cumpre papel primordial para que tudo funcione. Os riscos encontrados nesses ativos são exatamente os mesmos encontrados em qualquer infraestrutura de TI análoga. Está sujeita a acessos indevidos, modificação de dados, indisponibilidade de informações, etc. A lista é grande.

Desse modo, as recomendações de segurança são compartilhadas com qualquer infraestrutura de TI:

- Criptografar a informação sensível armazenada na nuvem.
- Utilizar, sempre que possível, comunicação criptografada.
- Utilizar certificados digitais para autenticação de dispositivos, lembrando que, em muitos casos, teremos uma comunicação M2M.
- Utilizar equipamentos de proteção de rede (firewall, IDS).
- Desativar serviços que não são necessários.
- Monitorar tráfego de dados.

As corporações sabem que cuidar da segurança de uma infraestrutura de TI não é tarefa fácil, e, quando nos voltamos para o ambiente residencial, é mais difícil ainda. Mesmo nesse ambiente, é possível realizar algumas ações para garantir sua própria segurança.

*"A essência do sucesso da tecnologia IoT está baseada justamente na capacidade de comunicação, troca de informações, armazenamento e disponibilidade de dados dos dispositivos"*

**APLICAÇÃO:** De um modo geral, as aplicações em IoT têm função gerencial, informativa e transacional. Elas utilizam os dados gerados/coletados pelos dispositivos para elaboração de gráficos, estatísticas, métricas, planos de trabalho, bilhetagem, BI, etc. Informações imprecisas sabidamente causam grandes transtornos e prejuízos, mas nesse ponto quero dar destaque especial a um tipo específico de aplicação, a de **CONTROLE**.

Ela pode atuar diretamente no device. Se levarmos em conta que ela pode controlar fechaduras, acionadores, motores, câmeras, equipamentos industriais, dispositivos de saúde e até carros inteligentes, passamos a ter uma visão do quanto é importante tratar cibersegurança em IoT.

Imagine situações hipotéticas na qual um cibercriminoso invade um marca-passos (já aconteceu) ou uma bomba de insulina de um paciente ou ainda a central de controle de um carro. Ele pode modificar os parâmetros que desejar. Chegamos então ao cerne da discussão sobre segurança em IoT:

Essa tecnologia, em um futuro próximo, em casos extremos, pode até matar!

É para se assustar? Sim! Mas não devemos deixar de utilizar a tecnologia por esse motivo. Cabe a nós, profissionais que lidam diariamente com cibersegurança, trabalhar e desenvolver processos e ferramentas capazes de garantir o uso seguro da IoT. As possibilidades são inúmeras e os benefícios que a tecnologia nos traz também. A cibersegurança em IoT tem um longo caminho (sem volta) que precisa ser trilhado!

1 Arduino é uma plataforma eletrônica open-source baseada na facilidade de implementação de hardware e software. Mais informações em www.arduino.cc.

Arquivo pessoal

# Cibersegurança: uma reflexão sobre a educação digital à luz do Direito


**Renato Gomes de Mattos Malafaia**

*Advogado especializado em Direito Digital no escritório Opice Blum, Bruno, Abrusio e Vainzof Advogados, bacharel em Direito pela Universidade Presbiteriana Mackenzie, pós-graduando em Direito e Tecnologia da Informação pela Escola Politécnica de Engenharia da Universidade de São Paulo. Membro do Comitê de Estudos em Compliance Digital da Legal, Ethics and Compliance (LEC) e da Comissão Permanente de Estudos de Tecnologia e Informação do Instituto dos Advogados de São Paulo (Iasp).*


O avanço tecnológico trouxe mudanças emblemáticas nas relações sociais e profissionais, em todos os ramos da vida cotidiana. Nesse novo cenário, cidadãos se tornaram internautas, opiniões pessoais se disseminaram em posts e dados de clientes viraram bytes. Ninguém mais sobrevive sem um computador pessoal.

Naturalmente, os ilícitos que costumavam ser praticados somente pela via presencial também migraram para o mundo digital e, ali instalados, passaram a aprimorar cada vez mais sua forma de execução. Exemplo disso é a exploração do uso do e-mail – principal forma de comunicação a distância durante alguns anos – para a prática generalizada de phishing, fraude digital em que o agente tenta se valer de imagens, pessoas ou assuntos relevantes para direcionar suas vítimas a instalar vulnerabilidades em sua máquina ou acessar sites falsos, desenvolvidos com o propósito específico de induzi-las a fornecer dados sensíveis (como credenciais de acesso), para permitir o uso ilícito pelo infrator.

Com o crescimento exponencial do uso de aplicativos de troca de mensagens instantâneas, estamos presenciando esse tipo de prática ser aprimorada para migrar para essas novas ferramentas de comunicação. Quem nunca recebeu uma mensagem via Whatsapp enviada por alguém que se fazia passar por uma instituição financeira?

Mais recentemente, o mundo testemunhou uma série de ataques cibernéticos destinados a criptografar arquivos do computador por meio de vírus espalhados na internet que atingem falhas do sistema operacional do dispositivo vítima. Conhecida como ransomware, a prática objetiva impossibilitar o uso dos dados nos computadores e redes infectados, como se os sequestrasse, pedindo contraprestação pecuniária para desbloqueio dos dados. Somente no ano de 2017, o ataque atingiu hospitais, sistemas de trans-

porte público e incontáveis empresas do setor privado, muitas das quais chegaram a parar as próprias operações.

Como se observa, o mundo digital atrai interesse não só de usuários que fazem o uso legítimo da grande rede, mas também de fraudadores e outros tipos de agentes que buscam se aproveitar do suposto anonimato propiciado pela rede para praticarem ilícitos.

A grande questão é que a inovação tecnológica corre em velocidade muito superior à produção legislativa. O Direito, como uma ciência eminentemente social, tenta acompanhar os litígios decorrentes do avanço tecnológico, mas, evidentemente, não consegue prever e disciplinar de antemão todos os pontos do progresso tecnológico que demandarão regulamentação.

No Brasil, são várias as iniciativas para adequar a legislação a esse novo mundo digital. No ano de 2012, foi inserido no Código Penal o crime de invasão de dispositivo informático, em decorrência do episódio vivido por famosa atriz que viu suas fotos íntimas indevidamente acessadas e publicadas na internet, sem o próprio consentimento. Naquele momento, a conduta virtual dos responsáveis por acessar indevidamente os arquivos da atriz não encontrava previsão na legislação criminal.

Posteriormente, o escândalo de espionagem de usuários brasileiros pelo governo americano, deflagrado pelas denúncias de Edward Snowden em junho de 2013, acabou por fomentar o debate acerca do então projeto de lei sobre princípios, garantias, direitos e deveres para o uso da internet, que acabou sancionado em 2014 pela então presidente da República Dilma Rousseffe recebeu o nome de Marco Civil da Internet.

Mais recentemente, influenciada pela crise econômica, a reforma trabalhista alterou a Consolidação das Leis do Trabalho, para incluir disposições relativas ao teletrabalho, considerado pela lei como a prestação de serviços fora das dependências do empregador, com a utilização de tecnologias de informação e comunicação.

Existem projetos de lei que pretendem criminalizar a divulgação e a exposição pública da intimidade sexual não autorizada – o tão corriqueiro vazamento de nudes – e até mesmo tipificá-las como uma nova forma de violência doméstica contra a mulher, com a inclusão dessas condutas na Lei Maria da Penha.

O que se nota é que o Direito vai se amoldando às novas ferramentas digitais, para aperfeiçoar a interpretação das disposições já constantes do ordenamento jurídico e aprovar leis específicas a esse novo universo, quando as demais não garantirem a necessária disciplina. Esse desafio de adaptar a legislação para contemplar os avanços tecnológicos não é apenas do Brasil, mas de países pelo mundo inteiro.

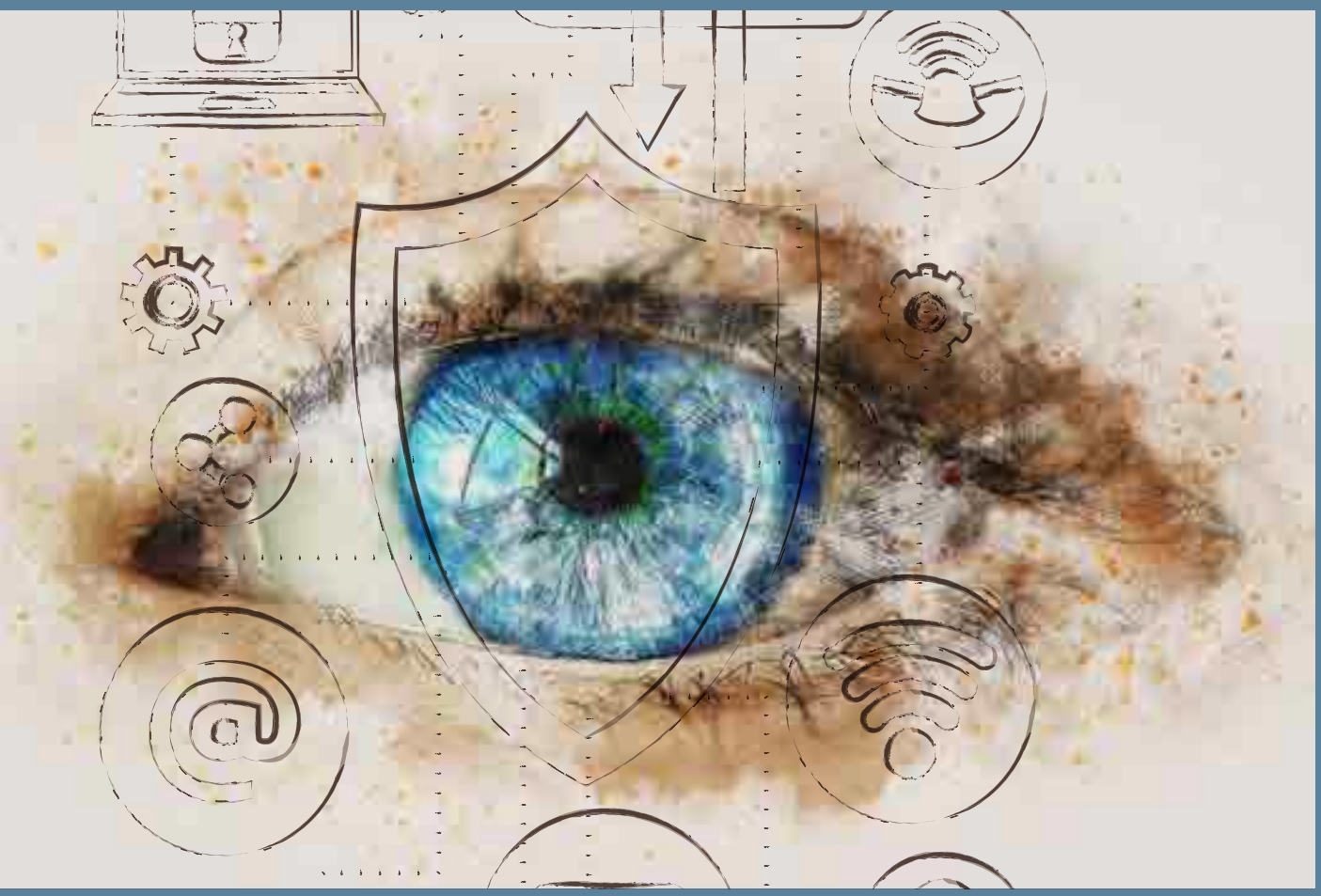
> ***"Não basta implementar tecnologias de última geração ou penalizar condutas tidas como inadmissíveis pela sociedade, se os usuários não tiverem o necessário conhecimento para manuseá-las"***

Portanto, a idealização da segurança cibernética transcende os aspectos exclusivamente técnicos ou jurídicos que circundam as tecnologias disponíveis aos usuários. Embora existam ferramentas que garantam elevadíssimo nível técnico de segurança e leis que reprimem condutas irregulares, a educação do usuário para agir de forma consciente e segura no mundo digital é fator fundamental para a cibersegurança.

Como se vê, não basta implementar tecnologias de última geração ou penalizar condutas tidas como inadmissíveis pela sociedade, se os usuários não tiverem o necessário conhecimento para manuseá-las. Diversos ataques cibernéticos, especialmente os de ransomware, poderiam ter sido evitados se os colaboradores de empresas tivessem os necessários conhecimentos sobre como interagir na rede.

Nessa toada, o próprio Marco Civil da Internet impôs ao Poder Público, em conjunto com os provedores de serviços de internet e a sociedade civil, a responsabilidade por promover a educação e fornecer informações sobre o uso dos programas de computador de controle parental, bem como para a definição de boas práticas para a inclusão digital de crianças e adolescentes.

Assim, a educação digital – seja da criança no âmbito familiar, seja do colaborador no ambiente corporativo – acerca da correta utilização dos recursos tecnológicos é fulcral para mitigar riscos cibernéticos a que estamos expostos nesse universo digital nos dias atuais. Precisamos nos preparar para hoje e para o futuro!



Os caminhos para a preparação dos profissionais e das organizações para os tempos atuais em que manter a segurança da informação é vital.

A história nos lembra de que ataques em que se aproveitaram da vulnerabilidade do oponente sempre existiram. E é dessa forma que agem os cibercriminosos atualmente: aproveitando-se da fragilidade e da insegurança alheias.

A conectividade do mundo moderno exige aplicações que permitam o compartilhamento de informações entre pessoas e entre empresas. É fundamental garantir a proteção dos dados para evitar a indisponibilidade deles por ataques cibernéticos.

A guerra cibernética, o desafio enfrentado pelas empresas e o que elas estão ou deveriam estar fazendo, efetivamente, para combater os ataques, num cenário complexo e assustador, mas que dispõe de farto material de apoio para tornar o ambiente empresarial mais seguro.

A tecnologia blockchain como aliada da votação por meios eletrônicos, garantindo confiabilidade, integralidade e confidencialidade em qualquer eleição.

# Desenvolvimento de software seguro: como se proteger dos ataques cibernéticos?

Arquivo pessoal


## Alander Antônio Faustino

*MBA em Gestão de Segurança da Informação pela Fumec e bacharel em Sistemas de Informação pelo Centro Universitário do Leste de Minas Gerais. Certificado ISO 27002. Atua na área de tecnologia da informação há 18 anos. Atualmente, trabalha na Gerência de Segurança da Informação da Prodemge.*


Arquivo pessoal


## Juliana Alves de Paula

*Pós-graduada em Redes de Computadores pela Pontifícia Universidade Católica de Minas Gerais (PUC MG) e tecnológa em Processamento de Dados pela Faculdade Brasileira de Informática (Fabrai). Atua na área de tecnologia da informação desde 1999. Atualmente, trabalha na área de Tratamento de Incidentes e Operações de Segurança da Informação da Prodemge.*


Arquivo pessoal


## Wilderson Alves Garcia

*Pós-graduado em Segurança da Informação pelo Senac e bacharel em Sistemas de informação pela Anhanguera Educacional. Certificado ITIL v3. Atua na área de tecnologia da informação desde 1998 e na área de segurança da informação há 7 anos. Atualmente trabalha na área de Tratamentos de Incidentes e Operações de Segurança da Informação da Prodemge.*



### Resumo

*Este artigo trata dos aspectos de segurança a serem observados no processo de desenvolvimento de software. Em um mundo que anseia por conectividade, cada vez mais torna-se necessária a construção de aplicações que permitam viabilizar o compartilhamento de informações entre pessoas ou entre as empresas. E para garantir esta ação, a segurança da informação é a principal aliada quanto à adoção de mecanismos que permitam garantir a proteção dos dados, mitigar a exploração de vulnerabilidades e evitar a indisponibilidade por ataques cibernéticos.*



***Palavras-chave:***
*desenvolvimento seguro, internet, segurança, software.*


## 1. Introdução

Com a expansão da internet, a necessidade de conectividade e do desenvolvimento de aplicações web tem sido constante. Fatores como mobilidade, agilidade, escalabilidade, flexibilidade e comodidade justificam esse comportamento.

Ao longo dos anos, o desenvolvimento de software em si deixou de ser meramente um meio de automatizar processos de sistemas de informação ou processos de infraestrutura para algo muito maior, pois agora estamos lidando com grandes volumes de informações pessoais e de negócio.

De acordo com Holanda e Fernandes (2011), grande parte dos incidentes de segurança da informação tem como origem as vulnerabilidades presentes em softwares. A codificação puramente simples do desenvolvedor, quando o mesmo considera apenas os cenários positivos de

execução de um código, sem se preocupar com usuários maliciosos e suas atitudes, é um dos principais fatores causadores dessas vulnerabilidades.

Implementar a segurança no desenvolvimento tornou-se requisito obrigatório, uma vez que os incidentes causados a partir da exploração de vulnerabilidades de codificação em ataques cibernéticos quase sempre ocasionam a indisponibilidade de uma infraestrutura, a perda de integridade da aplicação ou a divulgação não autorizada da informação obtida indevidamente.

Segundo Uto e Melo (2009), prover a segurança de um software não é um objetivo fácil de ser alcançado devido à complexidade dos softwares desenvolvidos atualmente. Rapidamente milhares de linhas são codificadas, o que invariavelmente ocasiona uma quantidade significativa de defeitos que podem impactar diretamente a segurança da aplicação. Considera-se ainda que, normalmente, quando um ciclo de desenvolvimento de software seguro não é adotado, o resultado final são especificações inseguras e configuração vulnerável de plataformas subjacentes.

O objetivo deste artigo é apresentar considerações sobre o desenvolvimento seguro de software a partir das falhas e vulnerabilidades de codificação existentes, as metodologias mais utilizadas e suas características, além de frameworks e ferramentas relacionadas ao tema proposto.

## 2. Estatísticas relativas a ataques que exploram falhas de desenvolvimento

Ter uma infraestrutura robusta não significa necessariamente que um software é totalmente seguro. De nada adiantam proteções da rede como firewall, IDS, IPS, ou recursos como alta disponibilidade, controle de acesso com múltiplos fatores de autenticação e políticas de senhas fortes, se o software desenvolvido não possuir mecanismos que impeçam um usuário malicioso de realizar ataques a partir de uma entrada de dados em um formulário web.

Desenvolver um software totalmente seguro e que não necessite de atualizações ainda é um desafio grande para os desenvolvedores e para as empresas que os fornecem. Com a expansão da internet, os ataques cibernéticos passaram a ser mais direcionados às aplicações em detrimento dos sistemas operacionais. Em 2009, o relatório "The Top Cyber Security Risks", publicado pelo SANS Institute[1], já justificava essa tendência, ao demonstrar que ataques contra aplicações web constituíam mais de 60% do total das tentativas observadas na internet.

> [...] Durante os últimos anos, o número de vulnerabilidades descobertas em aplicações web tem sido muito maior do que o número de vulnerabilidades descobertas em sistemas operacionais e, como resultado, mais tentativas de exploração são registradas em aplicações web que em sistemas operacionais (HOLANDA; FERNANDES, 2011, p. 16).

Diversos institutos de segurança apresentam na internet listas atualizadas com os mais variados e frequentes tipos de ataque e vulnerabilidades em softwares. O Common Vulnerabilities and Exposures (CVE[2]), por exemplo, mantém uma listagem com o quantitativo de vulnerabilidades exploradas e seus respectivos detalhes desde o ano de 1999. Ao observar essa listagem percebe-se que o quantitativo de vulnerabilidades reportadas aumentou significativamente ao longo dos anos.

Nos últimos cinco anos, conforme tabela da p. 95 ao lado do CVE, podemos identificar que diversas vulnerabilidades (como, por exemplo, SQL Injection, XSS – Cross-Site-Scripting e CRSF – Cross-Site Request Forgery), que apresentaram redução no período de 2014 a 2016, neste ano já apresentaram crescimento, interrompendo a sequência de queda. Nesses casos, o número de vulnerabilidades reportadas quase triplicou. Até o final de 2017, a previsão é que esse quantitativo aumente consideravelmente.

A Trustwave (2017), em seu relatório de segurança publicado anualmente, apresentou dados alarmantes no que diz respeito à segurança das aplicações e ataques web para os anos de 2015 e 2016:

- 99,7% das aplicações web testadas apresentavam pelo menos uma vulnerabilidade.
- 77% das vulnerabilidades detectadas envolviam gerenciamento de sessão.
- 10% das vulnerabilidades foram classificadas como críticas ou de alto risco.
- 13% dos ataques realizados utilizaram Cross-Site Scripting (XSS).
- 11% das vulnerabilidades de redes detectadas estavam relacionadas a servidores de rede com protocolos SSL e TLS inseguros.
- O número médio de vulnerabilidades encontradas por aplicação é de 11 (onze) vulnerabilidades.

1 SANS – SANS (SysAdmin, Audit, Network, Security) Institute. Disponível em: www.sans.org . Acesso em: 20 set/2017.
2 Disponível em: www.cvedetails.com. Acesso em: set/2017.

**Tabela 1: Tipos de vulnerabilidade. Período jan/2013 – set/2017. (CVE, 2017)**

| | Ano | | | | |
|---|---|---|---|---|---|
| **Vulnerabilidades** | **2013** | **2014** | **2015** | **2016** | **2017** |
| DoS | 1454 | 1598 | 1792 | 2029 | 2504 |
| Code Execution | 1186 | 1574 | 1825 | 1494 | 2311 |
| Overflow | 859 | 850 | 1079 | 1326 | 2151 |
| Memory Corruption | 366 | 420 | 749 | 717 | 542 |
| SQL Injection | 156 | 305 | 217 | 94 | 287 |
| XSS | 650 | 1105 | 776 | 497 | 1116 |
| Directory Traversal | 110 | 204 | 149 | 99 | 214 |
| Http Response Splitting | 7 | 12 | 12 | 15 | 8 |
| Bypass something | 352 | 457 | 577 | 446 | 462 |
| Gain information | 511 | 2104 | 748 | 843 | 1248 |
| Gain Privileges | 274 | 239 | 367 | 601 | 357 |
| CSRF | 123 | 264 | 248 | 87 | 254 |
| File Inclusion | 1 | 2 | 5 | 7 | 16 |

O Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (Cert.br) recebe notificações voluntárias de incidentes de segurança de todo os Grupos de Resposta a Incidentes de Segurança (CSIRT) do país. Após consolidar todos os incidentes enviados ao longo do ano de 2016, a seguinte análise foi apresentada (Cert.br, 2016). (Ver tabela na p.96)

## 3. OWASP

O OWASP (Open Web Application Security Project), ou Projeto Aberto de Segurança em Aplicações Web, é uma comunidade on-line que tem como objetivo criar e disponibilizar, de forma gratuita, artigos, metodologias, documentação, ferramentas e tecnologias no que diz respeito à segurança das aplicações web (SOUZA, 2017). É considerado um dos principais fomentadores das iniciativas relacionadas ao processo de desenvolvimento de aplicações seguras e mitigação de vulnerabilidades.

O trabalho conhecido como OWASP Top 10 tem como objetivo promover a sensibilização sobre segurança em aplicações por meio da identificação dos riscos mais críticos enfrentados pelas organizações. A última versão oficial é a de 2013, uma vez que a versão 2017 ainda está em apreciação para publicação.

A listagem com os 10 mais críticos riscos de segurança em aplicações web (Top Ten Most Critical Web Application Security Risk) é composta por (OWASP, 2013):

1) **Injeção:** as falhas de injeção, tais como injeção de SQL, de Sistema Operacional e de LDAP, ocorrem quando dados não confiáveis são enviados para um interpretador como parte de um comando ou consulta. Os dados manipulados pelo atacante podem iludir o interpretador para que este execute comandos indesejados ou permita o acesso a dados não autorizados.

2) **Quebra de autenticação e gerenciamento de sessão:** as funções da aplicação relacionadas com autenticação e gerenciamento de sessão geralmente são implementadas de forma incorreta, permitindo que os atacantes comprometam senhas, chaves e tokens de sessão ou, ainda, explorem outra falha da implementação para assumir a identidade de outros usuários.

3) **Cross-Site Scripting (XSS):** falhas XSS ocorrem sempre que uma aplicação recebe dados não confiáveis e os envia ao navegador sem validação ou filtro adequados. XSS permite aos atacantes executarem scripts no navegador da vítima que podem "sequestrar" sessões do usuário, desfigurar sites ou redirecionar o usuário para sites maliciosos.

4) **Referência insegura e direta a objetos:** uma referência insegura e direta a um objeto ocorre quando um programador expõe uma referência à implementação interna de um objeto, como um arquivo, diretório ou registro da base de dados. Sem a verificação do controle de acesso ou outra proteção, os atacantes podem manipular essas referências para acessar dados não autorizados.

3 LDAP - Lightweight Directory Access Protocol.

**Tabela 2: Consolidado sobre a análise de fatos de interesse apresentados pelo Cert.br quanto ao quantitativo de incidentes reportados ao longo do ano de 2016 (Cert.br, 2016. Adaptado).**

| Fato de interesse | Considerações |
|---|---|
| Ataques de negação de serviço | • No ano de 2016, foram 60.432 notificações de computadores que participaram de ataques de negação de serviço (DoS). Um aumento de 138% em comparação a 2015.<br>• A maior parte das notificações corresponde a ataques originados por equipamentos de IoT (internet das coisas) que estavam infectados e participantes de botnets.<br>• Houve uma queda sensível de ataques de negação de serviço que envolvam protocolos de rede, como, por exemplo, CHARGEN (19/UDP), DNS (53/UDP), NTP (123/UDP), SNMP (161/UDP) e SSDP (1900/UDP). |
| Tentativas de fraude | • Em 2016, foram 102.718 notificações de tentativas de fraude. Em comparação a 2015, houve queda de 39%.<br>• Em compensação, os casos de páginas falsas de bancos e comércio eletrônico aumentaram 37% em relação a 2015.<br>• Notificações sobre Cavalos de Troia tiveram queda de 46% em relação a 2015.<br>• Notificações sobre eventuais quebras de direitos autorais foram 99% menores em relação a 2015. |
| Varreduras e propagação de códigos maliciosos | • Notificações de varreduras, em 2016, mantiveram-se nos mesmos patamares de 2015, com pequena redução de 2%. Foram 383.903 em 2016.<br>• Alguns serviços como TELNET, SSH, FTP e RDP, que são costumeiramente alvos de ataques de força bruta, continuam visados.<br>• Varreduras de TELNET, que apresentaram destaque em 2015, estão visando a dispositivos IoT e equipamentos de rede residenciais, tais como modens ADSL e cabo, roteadores wi-fi, etc.<br>• Varreduras de SMTP corresponderam a 30% de todas as notificações de varreduras em 2016. Em 2015, esse número foi de 7%. As varreduras desse SMTP estão relacionadas a três tipos de abuso: tentativa de envios de e-mails utilizando ataques de dicionário de nomes de usuários, exploração de servidores de e-mail e ataques de força bruta utilizando credenciais descobertas de usuários. |
| Ataques a servidores web | • Em 2016, foram realizadas 55.441 notificações de ataques a servidores web. Em comparação a 2015, uma redução de 16%.<br>• Atacantes exploram vulnerabilidades em aplicações web para comprometê-las e realizar atividades indevidas, tais como: hospedagem de página falsa, armazenamento de ferramentas de ataque e propagação de spam.<br>• Foram observadas ainda diversas notificações de ataques de força bruta contra sistemas de gerenciamento de conteúdo, como WordPress e Joomla. Os ataques em questão constituíam na grande maioria em tentativas de descoberta da senha de administrador desses sistemas. |
| Computadores comprometidos | • No ano de 2016, foram realizadas 1.695 notificações de computadores comprometidos. Em comparação a 2015, houve redução de 31%.<br>• A maior parte do montante de notificações de comprometimento foi referente a servidores web que tiveram suas páginas desfiguradas (defacement). |
| Outros incidentes | Foram 14.675 notificações em 2016 que se enquadram na categoria "outros", correspondendo a um número 30% menor que o total registrado em 2015. |

5) **Configuração incorreta de segurança:** uma boa segurança exige a definição de uma configuração segura e implementada na aplicação, frameworks, servidor de aplicação, servidor web, bancos de dados e plataforma. Todas essas configurações devem ser definidas, implementadas e mantidas, já que geralmente a configuração padrão é insegura. Adicionalmente, o software deve ser mantido atualizado.

6) **Exposição de dados sensíveis:** muitas aplicações web não protegem devidamente os dados sensíveis, tais como cartões de crédito, IDs fiscais e credenciais de autenticação. Os atacantes podem roubar ou modificar esses dados desprotegidos com o propósito de realizar fraudes de cartões de crédito, roubo de identidade ou outros crimes. Os dados sensíveis merecem proteção extra, como criptografia no armazenamento ou em trânsito, bem como precauções especiais quando trafegadas pelo navegador.

7) **Falta de função para controle do nível de acesso:** a maioria das aplicações web verifica os direitos de acesso em nível de função antes de tornar essa funcionalidade visível na interface do usuário. No entanto, as aplicações precisam executar as mesmas verificações de controle de acesso no servidor quando cada função é invocada. Se essas requisições não forem verificadas, os atacantes serão capazes de forjar as requisições, com o propósito de acessar a funcionalidade sem autorização adequada.

8) **Cross-Site Request Forgery (CSRF):** um ataque CSRF força a vítima que possui uma sessão ativa em um navegador a enviar uma requisição HTTP forjada, incluindo o cookie da sessão da vítima e qualquer outra informação de autenticação incluída na sessão, a uma aplicação web vulnerável. Essa falha permite ao atacante forçar o navegador da vítima a criar requisições que a aplicação vulnerável aceite como requisições legítimas realizadas pela vítima.

9) **Utilização de componentes vulneráveis conhecidos:** componentes tais como bibliotecas, frameworks e outros módulos de software quase sempre são executados com privilégios elevados. Se um componente vulnerável é explorado, um ataque pode causar sérias perdas de dados ou comprometer o servidor. As aplicações que utilizam componentes com vulnerabilidades conhecidas podem minar as suas defesas e permitir uma gama de possíveis ataques e impactos.

10) **Redirecionamentos e encaminhamentos inválidos:** aplicações web frequentemente redirecionam e encaminham usuários para outras páginas e sites e usam dados não confiáveis para determinar as páginas de destino. Sem uma validação adequada, os atacantes podem redirecionar as vítimas para sites de phishing ou malware ou usar encaminhamentos para acessar páginas não autorizadas.

## 4. Ciclo de desenvolvimento de software seguro

### 4.1. Custo, prazo e planejamento inadequado: inimigos da segurança?

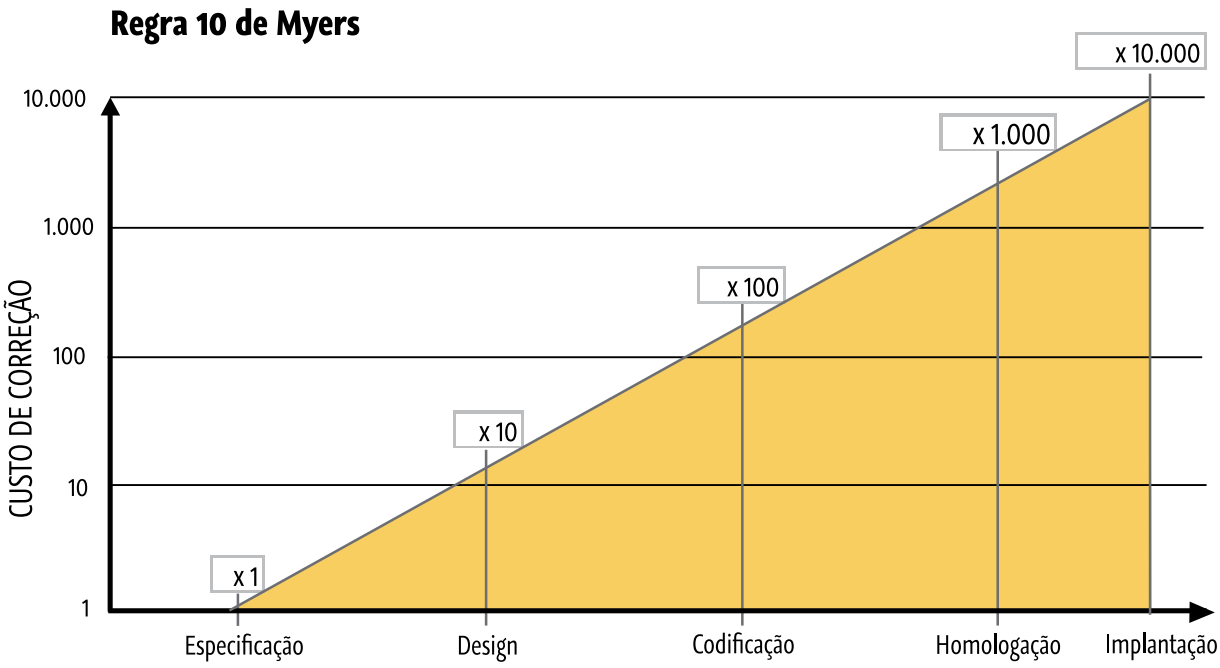
A partir do momento em que os softwares são disponibilizados para acesso por meio da internet, os mesmos estão sujeitos a todo tipo de ataque cujo objetivo é a exploração de falhas e vulnerabilidades de codificação.

Segundo Uto e Melo (2009), um software seguro é aquele que consegue satisfazer os requisitos de segurança em condições normais de operação e em situações decorrentes de atividade maliciosa. Para atender esse objetivo, o mesmo deve ser resultado de um ciclo de desenvolvimento que considerou requisitos de segurança em todas as etapas, desde a especificação até a implantação em produção.

Porém, na maioria dos casos, esse objetivo não é alcançado, pois o prazo de desenvolvimento é definido pela área comercial para atender as demandas e necessidades do mercado ou de um cliente em específico. A pressão pelo cumprimento desses prazos faz com que os requisitos de segurança só sejam aplicados ao final do processo durante os testes e nas validações finais antes de serem publicados em produção. Como as equipes de desenvolvimento não planejam e nem se preocupam com requisitos de segurança, desde o início do processo, ocorre um grande impacto no produto final, resultando em um software sem segurança e com um significativo número de vulnerabilidades capazes de serem exploradas em ataques cibernéticos. A necessidade de aplicar as correções de segurança a essas vulnerabilidades depois do software pronto acaba prejudicando todo o planejamento, pois afeta diretamente o custo e o tempo de construção anteriormente estipulado.

Em 1979, o renomado autor e cientista da computação Glendford Myers em seu livro *The Art of Software Testing* (A arte do teste de software), apresentava o conceito de que o custo de uma manutenção tende a ser 10 vezes maior a cada ciclo de vida do desenvolvimento. Esse conceito ficou conhecido como a "Regra 10 de Myers". A teoria descrita por Myers, apesar de possuir quase 40 anos, ainda é considerada regra essencial no processo de desenvolvimento.

**Figura 1 - Regra 10 de Myers (Inmetrics, 2016. Adaptado).**




O custo de um software seguro diminui quando os critérios de segurança estão claramente descritos desde o início (ISO/IEC 27002, 2013). Cada etapa do ciclo de desenvolvimento de um software tem sua contribuição de segurança para a qualidade do produto final a ser entregue e, portanto, não pode ser omitida durante esse processo. Por isso se faz importante que ainda na fase de especificação os requisitos funcionais e de segurança sejam avaliados, para que, ao final do processo de desenvolvimento, as chances de vulnerabilidades sejam mínimas ou inexistentes.

### 4.2. Metodologias de desenvolvimento seguro

Para uma empresa ou para uma equipe de desenvolvimento que tem como objetivo atingir a maturidade no processo de codificação segura, é fundamental a adoção de um modelo ou de uma metodologia estruturada. Uma metodologia de desenvolvimento voltada para a segurança deve incluir necessariamente os seguintes atributos (Wiesmann *et al.*, 2005):

- Facilidade de adaptação quanto a design, testes e documentação;
- Atividades que permitam que controles de segurança (tais como análise de risco, ameaças, revisões de código, etc.) possam ser aplicados;
- Métricas capazes de auxiliar o aumento do nível de maturidade de segurança da organização e;
- Potencial para redução das taxas de erros correntes, e melhorar a produtividade do desenvolvimento.

Já a OWASP (2010) recomenda as seguintes práticas:

- Definição clara dos papéis e responsabilidades;
- Equipes de desenvolvimento com formação adequada em segurança no processo de desenvolvimento de aplicações;
- Implementação de ciclo de desenvolvimento de software seguro;
- Definição de padrões de programação segura;
- Construção de bibliotecas reutilizáveis ou utilização de uma biblioteca de segurança;
- Verificação da efetividade dos controles de segurança;
- Definição de práticas para garantir a segurança quando há terceirização no desenvolvimento, com a inclusão dos requisitos de segurança e metodologias definidas.

Dentre os modelos mais conhecidos de desenvolvimento seguro, destacam-se o SDL (Secure Development Lifecycle) da Microsoft e o CLASP (Comprehensive, Lightweight Application Security Project) do OWASP, que serão descritos a seguir.

### 4.2.1. SDL – Security Development Lifecycle

Segundo Howard e Lipner (2005) e Microsoft (2010), o Security Development Lifecycle (SDL) é um processo de desenvolvimento de software com segurança que é adotado pela Microsoft em seus produtos. Aberto a qualquer plataforma, possui todo o seu conteúdo publicado para consulta. O SDL tem como objetivo introduzir medidas de segurança e privacidade em todas as etapas do processo de desenvolvimento e por meio da integração dessas medidas obter um software seguro como produto final, adicionando pontos de verificação e produtos de segurança bem definidos.

O processo de desenvolvimento de software seguro proposto pela Microsoft é composto pelas seguintes etapas: treinamento, requisitos, design, implementação, verificação, lançamento e resposta, conforme demonstrado na figura 2.

Descrição das fases do processo de desenvolvimento padrão (SDL Simplificado MICROSOFT, 2010):

**Treinamento (fase de pré-requisito)**

Na fase de treinamento, toda a equipe de desenvolvimento recebe treinamentos de segurança básicos e avançados que aborda aspectos como princípios e tendências em segurança e privacidade.

O treinamento deve compreender conceitos fundamentais, como:

**a)** Design de segurança;

**b)** Modelagem de ameaças;

**c)** Codificação de segurança;

**d)** Testes de segurança;

**e)** privacidade.

**Requisitos (fase um)**

Nesta fase, todos os requisitos de segurança e privacidade são avaliados de forma detalhada. É produzida uma análise de custos que avalia se os recursos necessários para melhorar a segurança e a privacidade estão compatíveis com os objetivos de negócio do software a ser desenvolvido. Essa fase é uma oportunidade para a equipe do produto considerar como a segurança será integrada no processo de desenvolvimento, identificar os objetivos-chave de segurança e maximizar a segurança do software, minimizando a quebra de planos e cronogramas.

**Design (fase dois)**

A fase de design identifica a estrutura e os requisitos gerais do software. Nessa fase, é realizada a análise da superfície de ataque da aplicação, na qual serão especificados quais os recursos de segurança e privacidade serão expostos ao usuário. Depois dessa análise, ocorre a redução da superfície de ataque, aplicando-se conceitos de segurança, como privilégio mínimo e defesa em camadas. Por fim, é

**Figura 2 - Microsoft Security Development Lifecycle (SDL) (MICROSOFT, 2010. Simplificado).**

produzido um modelo de ameaças que permite que as equipes de desenvolvimento identifiquem as implicações de segurança de forma estruturada relativamente a componente e aplicativo, reduzindo a possibilidade de vulnerabilidades.

**Implementação (fase três)**

Na fase de implementação, a equipe do produto gera o código, testa e integra o software. São empregadas técnicas de programação defensiva (também conhecida como codificação segura), na qual o código produzido é capaz de resistir a ataques de usuários maliciosos. Também são adotados padrões de codificação que reduzem a ocorrência de vulnerabilidades. De acordo com Howard e Lipner (2005), a etapa de realização de revisão de códigos é essencial para a remoção de vulnerabilidades no processo de desenvolvimento de software.

**Verificação (fase quatro)**

Nesta fase, ocorre a análise de documentação do software, a inspeção de código e a realização de testes por meio de ferramentas automatizadas, como, por exemplo, de análise estática de código ou de testes manuais para identificar partes da codificação construída que estejam suscetíveis à introdução de vulnerabilidades. Realizar um esforço de segurança durante a fase de verificação é realmente uma prática recomendada para garantir que o software final preencha os requisitos e permita uma revisão mais profunda do código herdado que tenha sido transferido nas versões anteriores do software.

Ressalta-se que as revisões de código e os testes de código de alta prioridade (aqueles que são parte da "superfície de ataque" dos softwares) ocorridos nessa fase são extremamente críticos para as demais partes do SDL.

**Liberação ou release (fase cinco)**

Na fase de liberação ou release é que ocorre a produção do plano de ação que tem como objetivo a resposta a incidentes de segurança. Ainda que um software seja considerado seguro, o mesmo precisa de um plano de resposta principalmente quanto ao surgimento de novas ameaças.

Posteriormente, é realizada a revisão final de segurança e somente após essa revisão, na qual é confirmado que todos os requisitos de segurança e privacidade foram construídos conforme a especificação inicial, o software é liberado para produção.

**Resposta (fase pós-produção)**

Nesta fase ocorre a execução propriamente dita do plano de ação elaborado na fase de liberação.

As outras atividades de segurança, como revisão manual de código, teste de penetração ou análise de vulnerabilidades, são consideradas opcionais e somente serão executadas se a equipe de desenvolvimento ou a equipe de segurança acharem necessário.

### 4.2.2. Clasp – Comprehensive, Lightweight Application Security Process

Desenvolvido inicialmente pela empresa Secure Software, o Clasp (Comprehensive, Lightweight Application Security Process), hoje está sob a responsabilidade da OWASP. O Clasp é um conjunto de componentes de processo dirigidos por atividades e baseado em regras que articulam práticas para a construção de software seguro, fazendo com que o ciclo de vida de desenvolvimento de software SDLC (Software Development Life Cicle) possa ocorrer de maneira estruturada com repetição e mensuração.

Segundo o OWASP (2011), o Clasp pode ser descrito como um conjunto de pedaços de processos que podem ser utilizados em qualquer processo de desenvolvimento de software. Projetado para ser de fácil utilização, nele são documentadas todas as atividades que as organizações devem realizar, proporcionando, assim, uma extensa riqueza de recursos de segurança, facilitando a implementação dessas atividades.

O processo de desenvolvimento seguro Clasp é organizado conforme a estrutura a seguir.

**Visões Clasp**

O Clasp pode ser analisado por meio de perspectivas de alto nível chamadas Visões Clasp. As visões se dividem em: visão conceitual, visão baseada em regras, visão de avaliação de atividades, visão de implementação de atividades e visão de vulnerabilidade.

A visão conceitual (I) apresenta, de forma geral, como é o funcionamento do processo Clasp e a interação entre seus componentes. Nela são introduzidas as melhores práticas, a interação entre o Clasp e as políticas de segurança, os componentes do processo e alguns conceitos de segurança.

A visão baseada em regras (II) estabelece as responsabilidades mínimas de cada membro do projeto (gerente, arquiteto, especificador de requisitos, projetista, implementador, analista de testes e auditor de segurança), relacionando cada um deles com as atividades propostas, como também especifica quais são os requerimentos básicos de cada função.

A visão de avaliação (III) descreve o objetivo de cada atividade, quais são os custos para a implementação, a aplicabilidade, os impactos, além dos riscos, caso alguma atividade não seja realizada.

A visão de implementação (IV) descreve o conteúdo das 24 atividades de segurança definidas pelo Clasp, além de identificar os responsáveis para implementar cada atividade.

A visão de vulnerabilidades (V) apresenta um catálogo com a descrição de 104 tipos de vulnerabilidades no desenvolvimento de software, divididas em cinco categorias: erros de tipo e limites de tamanho, problemas do ambiente, erros de sincronização e temporização, erros de protocolo e erros lógicos em geral. Também são realizadas técnicas de mitigação e avaliação de risco.

**Recursos Clasp**

O Clasp suporta planejamento, implementação e desempenho para atividades de desenvolvimento de software relacionado com segurança. Os recursos do Clasp, compostos por uma lista de 11 artefatos, tem como objetivo fornecer acesso aos artefatos que serão de grande importância se o projeto estiver usando ferramentas para o processo Clasp. A tabela 3 (*página 102*) a seguir apresenta a lista de artefatos e com quais visões os recursos podem ser aplicados.

**Caso de uso de vulnerabilidade**

Os casos de uso de vulnerabilidades têm como objetivo descrever as condições nas quais os serviços de segurança possam se tornar vulneráveis, a partir de exemplos específicos e de fácil entendimento para o usuário. Relações de causa e efeito são utilizadas como uma metodologia na qual são apontados os resultados de exploração de vulnerabilidades em serviços básicos de

**Figura 3 - Visões Clasp. (OWASP, 2006 *apud* Holanda; Fernandes, 2011) (Adaptado).**

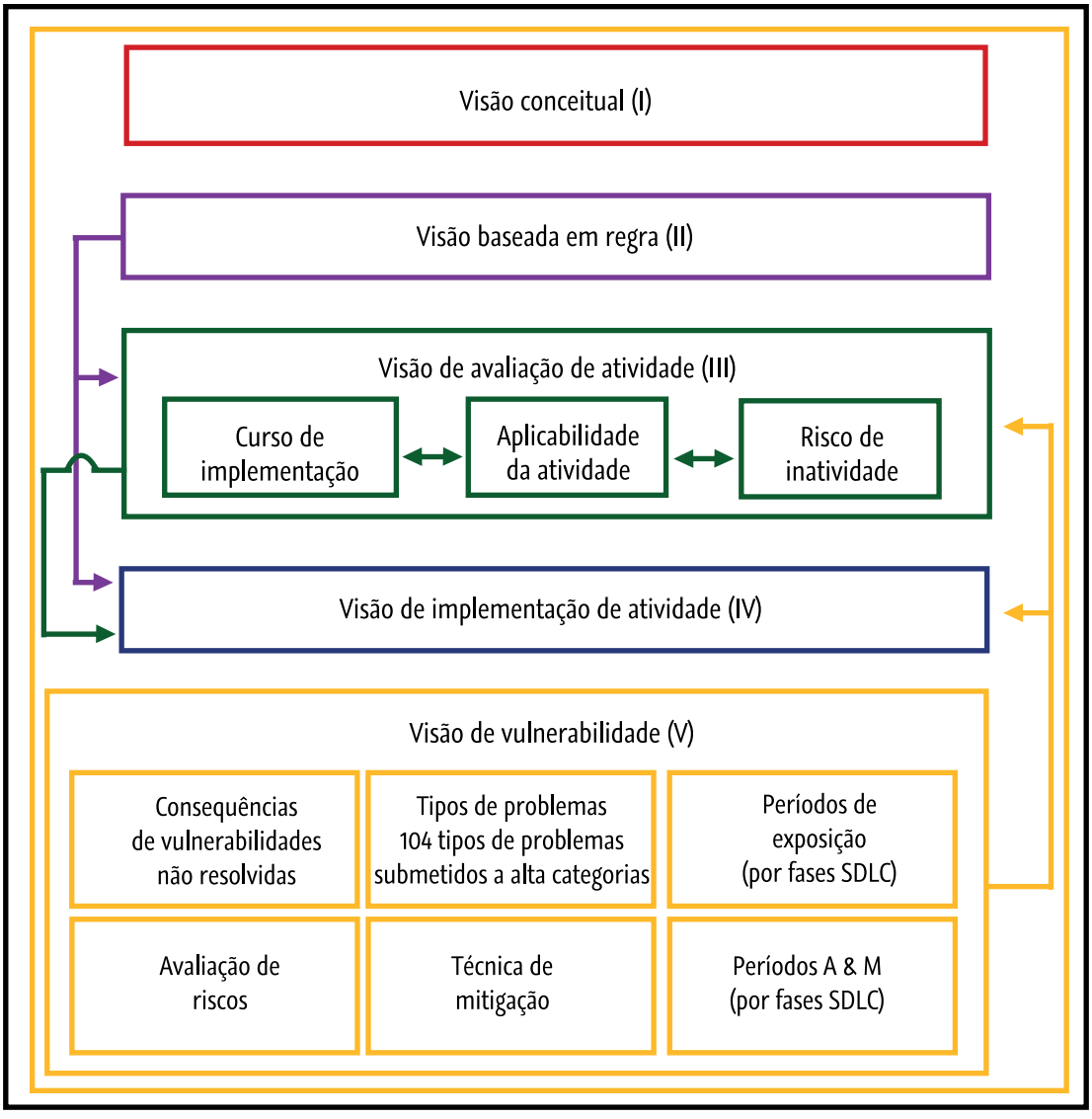


**Tabela 3: Lista de artefatos Clasp (OWASP, 2011. Adaptado).**

| ARTEFATOS | VISÕES |
|---|---|
| Princípios básicos em segurança de aplicações | Todas |
| Exemplos de princípios básicos: validação de entrada | Todas |
| Exemplos de princípios básicos: modelo de penetração | Todas |
| Serviços essenciais de segurança | III |
| Planilha com exemplos de codificação | II, III e IV |
| Planilha de avaliação de sistemas | III e IV |
| Mapa de caminho exemplo: projeto legado | III |
| Mapa de caminho exemplo: novo projeto | III |
| Plano de engenharia de processo | III |
| Formação de equipe | III |
| Glossário equipe de segurança | Todas |

segurança como autorização, autenticação, confidencialidade, disponibilidade, entre outros.

#### 4.2.3. Comparativo entre Clasp e SDL

Segundo Marques (2014), o modelo Clasp do OWASP veio para atender a necessidades de desenvolvimento de aplicações seguras onde a aplicação de modelos extensos e complexos, como o SDL da Microsoft, não era viável, seja pela ausência de recursos, pela acentuada curva de aprendizado dos modelos, seja pela falta de necessidade, em virtude do tamanho da organização.

Segundo Cividanes (2009), o SDL é totalmente voltado para a segurança e tem a necessidade de possuir uma equipe especialista em segurança da informação para acompanhar os processos definidos desse modelo durante o processo de desenvolvimento, além da equipe de codificação responsável pela construção da aplicação. A integração entre essas equipes não é apoiada, uma vez que a equipe de segurança é considerada totalmente responsável pela auditoria do documento do SDL durante o processo de desenvolvimento. Já o Clasp recomenda que as boas práticas e as atividades possam ser verificadas e revistas pela própria equipe de desenvolvimento.

Outra diferença significativa é que o SDL possui como foco somente o treinamento de desenvolvedores, enquanto o Clasp determina que os treinamentos de segurança incluam todas as equipes envolvidas no projeto.

### 4.3. Ferramentas e projetos de auxílio para atividades de codificação segura

A seguir, serão apresentadas algumas ferramentas e projetos que auxiliam no processo de codificação segura:

- **Application Security Verification Standard Project – ASVS[4] (OWASP):** o Application Security Verification Standard Project (ou Projeto de Padrões de Verificação de Segurança de Aplicações) é uma lista de requisitos de segurança e testes criada para auxiliar a equipe de desenvolvimento quanto à definição de uma aplicação segura. Tem como objetivo criar e estabelecer um framework de requerimentos de segurança e controles, que foca em normalizar os controles de segurança funcionais e não funcionais, melhorando o desenvolvimento e testes das aplicações.

- **Code Review Guide[5] (OWASP):** o *Code Review Guide* (Guia de Revisão de Código) é um livro técnico para desenvolvedores e profissionais de segurança, com foco em atividades de revisão de código e no estudo de vulnerabilidades que surgem ao longo do processo de desenvolvimento. O *Code Review Guide* não tem a intenção de mostrar como a empresa deve fazer as revisões de código dos sistemas que estão em desenvolvimento, e sim, apresentar termos genéricos e metodologias para que as empresas possam criar seus próprios padrões de verificação e integrá-los ao ciclo de vida de desenvolvimento seguro que a empresa já segue.

4 Disponível em: https://www.owasp.org/index.php/Category:OWASP_Application_Security_Verification_Standard_Project. Acesso em: set/2017.
5 Disponível em: https://www.owasp.org/index.php/Category:OWASP_Code_Review_Project. Acesso em: set/2017.

- **OWASP Enterprise Security API - Esapi[6]:** outra iniciativa da OWASP, a Enterprise Security API Toolkits é uma biblioteca de controles de segurança para aplicações web que auxiliam o desenvolvedor na construção de aplicações seguras e de baixo risco. É composta por um conjunto de classes encapsuladas que contém a maior parte dos tratamentos de segurança que as aplicações necessitam, como autenticação, controle de acesso, validação de entrada de dados, codificação de saída de dados, criptografia, configurações de segurança, entre outras funções.

- **OWASP WAP[7] – Web Application Protection Project:** o WAP é uma ferramenta de segurança que utiliza a análise estática do código-fonte para detectar vulnerabilidades, mineração de dados para prever falsos positivos e realiza correção do código fonte.

- **Software Assurance Metrics and Tools Evaluation – Samate[8] (NIST):** criado pelo National Institute of Standards and Tecnology – NIST, o Samate é um projeto dedicado a garantir a melhoria do software no governo americano, desenvolvendo métodos para validação de ferramentas de codificação e testes. As ferramentas são avaliadas, e caso aprovadas, são recomendadas para utilização dos desenvolvedores e parceiros responsáveis pela construção de softwares para o governo americano.

- **Cert Secure Coding Initiative[9] (Carnegie Mellon University):** o Cert Secure Coding Initiative é uma iniciativa financiada pelo governo americano que apresenta diversas definições quanto a padrões de codificação segura para linguagens como Java, C e C++, laboratórios para avaliação de conformidade, ferramentas de análise estática, entre outros.

- **Threat Modeling Tool[10] (Microsoft):** Threat Modeling Tool é uma ferramenta que permite realizar a modelagem de ameaças no processo de desenvolvimento seguro. A partir da modelagem de ameaças, é possível averiguar problemas de segurança com antecedência, quando ainda são relativamente fáceis e econômicos de serem resolvidos, auxiliando na redução do custo final da aplicação desenvolvida.

- **Rips[11] (Ripstech):** o Rips é uma ferramenta de análise estática de código para verificar vulnerabilidades em aplicações PHP. Em sua análise, consegue transformar o código-fonte em um modelo de programa para detecção de funções potencialmente vulneráveis e que podem ser exploradas por um usuário malicioso.

- **SonarQube[12] (Sonarsource):** mais conhecida como Sonar, o Sonarqube é uma ferramenta de gerenciamento da qualidade do código construído sobre uma série de aspectos e indica as melhores práticas quanto ao desenvolvimento de uma determinada funcionalidade. Possui suporte a muitas linguagens e pode ser utilizada com outras ferramentas de automatização e de controle de versionamento de ambientes.

- **FindBugs[13] (University of Maryland):** ferramenta de análise estática para codificação Java, o FindBugs examina classes ou arquivos JAR com o objetivo de identificar vulnerabilidades a partir de uma lista de padrões de erros.

## 5. Conclusão

Este trabalho teve como objetivo elucidar alguns aspectos sobre o processo de desenvolvimento de software seguro, na qual foram apresentados, por meio de fundamentação teórica, o detalhamento das principais vulnerabilidades exploradas por meio de codificação não segura e das metodologias e ferramentas adotadas pelo mercado para mitigação dessas vulnerabilidades e proteção dos dados.

Desenvolver um software seguro não é uma tarefa simples. Para que esse objetivo seja alcançado, se faz em necessárias a avaliação e a implementação da segurança em todo o ciclo de vida de desenvolvimento. Sem falar na constante atualização e sensibilização dos envolvidos no processo e na matéria, de forma a entender as ameaças existentes e como combatê-las. A adoção dessas iniciativas proporcionará melhores produtos e minimizará a ocorrência de possibilidade de exploração de falhas que possam existir.

Informação é um ativo essencial para os negócios de uma empresa. Proteger esse ativo adequadamente, para evitar que o mesmo seja exposto e utilizado de forma indevida, é de suma importância, ainda que vivenciemos tempos de negócios cada vez mais interconectados.

6 Disponível em: https://www.owasp.org/index.php/Category:OWASP_Enterprise_Security_API. Acesso em: set/2017.
7 Disponível em: https://www.owasp.org/index.php/OWASP_WAP-Web_Application_Protection. Acesso em: set/2017.
8 Disponível em: https://samate.nist.gov/Main_Page.html. Acesso em: set/2017.
9 Disponível em: http://www.cert.org/secure-coding/. Acesso em: set/2017.
10 Disponível em: https://www.microsoft.com/en-us/sdl/adopt/threatmodeling.aspx. Acesso em: set/2017.
11 Disponível em: https://www.ripstech.com/. Acesso em: set/2017.
12 Disponível em: https://www.sonarqube.org/. Acesso em: set/2017.
13 Disponível em: http://findbugs.sourceforge.net/. Acesso em: set/2017.

**Referências**


CERT.BR. **Incidentes reportados ao CERT.br – janeiro a dezembro de 2016.** (2016). Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil**.** Disponível em: https://www.cert.br/stats/incidentes/2016-jan-dec/analise.html. Acessado em: 4 set. 2017.

CIVIDANES, Filipe. **Overview CLASP**. (2009). Disponível em: http://fcividanes.blogspot.com.br/2009/06/overview-clasp.html. Acessado em: 4 set. 2017.

CVE. **Vulnerabilities by type.** (2017). Disponível em: https://www.cvedetails.com/vulnerabilities-by-types.php. Acessado em: set. 2017.

HOLANDA, Maristela T.; FERNANDES, Jorge H. C. **Segurança no desenvolvimento de aplicações**. Gestão da Segurança da Informação e Comunicações. CEGSIC 2009-2011, 2011.

INMETRICS. **Quanto custa um defeito de software?** Disponível em: http://www.inmetrics.com.br/quanto-custa-um-defeito-de-software/. Acessado em: 11 set. 2017.

ISO/IEC 27002 – ABNT NBR ISO/IEC 27002 – **Tecnologia da Informação – Técnicas de Segurança – Código de Prática para controles de Segurança da Informação.** Segunda Edição, 2013.

LIPNER, Steve; HOWARD, Michael. **O ciclo de vida do desenvolvimento da segurança de computação confiável.** 2005. Disponível em: https://msdn.microsoft.com/pt-br/library/ms995349.aspx. Acessado em: 11 set. 2017.

MARQUES. Marcius M. **Abordagem Ontológica para Mitigação de Riscos em Aplicações Web.** Dissertação apresentada como requisito parcial para conclusão do Mestrado em Informática. (2014). Universidade de Brasília.

MICROSOFT. **Microsoft Security Development Lifecycle** – **Implementação simplificada do Microsoft SDL.** Microsoft Press, 2010.

OWASP. **Owasp Clasp Project**. (2011). Disponível em https://www.owasp.org/index.php/ Category: OWASP CLASP Project. Acessado em: 14 set. 2017.

OWASP. **OWASP TOP 10**. (2013). Disponível em: https://www.owasp.org/index.php/ Category: OWASP Top Ten Project. Acessado em: 20 set. 2017.

SANS. **SANS 2009: The Top Cyber Security Risks**. Disponível em: http://www.sans.org/top-cyber-security-risks/. Acessado em: 20 set. 2017.

SOUZA, Rafael F. **OWASP Top 10 2017 Release Candidate**. (2017). Disponível em: https://cipher.com/br/2017/04/16/owasp-top-10-2017-release-candidate/. Acessado em: 20 set. 2017.

TRUSTWAVE. **2017 Trustwave Global Security Report**. (2017). Disponível em: https://www.trustwave.com/Resources/Global-Security-Report-Archive/. Acessado em: set. 2017.

UTO, Nelson; MELO, Sandro P. **Vulnerabilidades em Aplicações Web e Mecanismos de Proteção.** (2009). Disponível em: http://www.lbd.dcc.ufmg.br/colecoes/sbseg/2009/044.pdf . Acessado em: 20 set. 2017.

WIESMANN, A.; VAN DER STOCK, A.; CURPHEY, M.; STIRBEI, R. **A guide to building secure web applications and web services.** (2005). The Open Web Application Security Project.

# Cybersecurity: prepare-se para o pior

Arquivo pessoal


## *Fernando Fonseca*

*Professor e instrutor da Antebellum Capacitação Profissional. Possui certificado CISSP-ISSAP, CISM, CHFI, ISMAS.*



### *Resumo*

*Manter a segurança da informação nas organizações tornou-se um exercício de guerra cibernética com o uso de equipes de ataque e defesa para descobrir as vulnerabilidades e aprimorar as contramedidas. Este artigo aborda os caminhos para a preparação dos profissionais e das organizações para estes novos tempos.*



***Palavras-chave:***
*cybersecurity, red team, blue team, ransomware, NIST, gartner, bitcoin.*


O que grandes empresas como TJX, Sony, Dropbox, LinkedIn, Tumblr, Evernote, sBay, JP Morgan Chase, Adobe, Verisign, RSA Security, Yahoo, Ashley Madison, Target e Equifax têm em comum? Todas foram protagonistas de uns dos maiores vazamentos de dados conhecidos no mundo, e a maioria desses vazamentos culminou na demissão do CIO e/ou CEO da empresa. No caso mais recente, o da Equifax, as ações da empresa despencaram de US$ 142 para US$ 92, ou seja, perderam 1/3 de seu valor entre o dia 7 de setembro de 2017, quando foi anunciado o vazamento, e o dia 15 de setembro deste ano, quando foram anunciadas as demissões do CSO e do CIO da empresa. No dia 26 de setembro, foi a vez de Rick Smith, CSO e chairman da empresa, ser demitido.

Apesar do início intimidador, a intenção deste artigo não é espalhar medo, incerteza e dúvida (FUD - Fear, Uncertainty and Doubt) para exaltar a área de segurança da informação, mas, sim, trazer uma reflexão realista sobre os riscos atuais. Utilizamos somente exemplos norte-americanos, porque as empresas de lá são obrigadas, por lei, a informar qualquer vazamento de dados de clientes. Como não temos nenhuma lei parecida no Brasil, as empresas aqui tratam sigilosamente todos os prejuízos relacionados a ataques cibernéticos. Esses só aparecem nas empresas com ações na bolsa, quando se tornam um fato relevante, ou no balanço da empresa. Na função de investigador forense, posso garantir que, no Brasil, ocorrem inúmeros incidentes graves de segurança, mas sobre os quais ninguém quer falar.

Existe uma famosa citação norte-americana que nos diz para esperar o melhor e preparar-se para o pior, mas o que é o melhor? Há alguns anos, eu costumava dizer, em minhas aulas, que a maior parte dos incidentes e danos na segurança da informação era causada por erros evitáveis, como o superaquecimento de uma sala-cofre ou um analista que, por descuido, apagava um diretório no servidor de produção achando estar na tela do servidor de testes. As prevenções contra esses incidentes não lembravam nem de longe o emocionante jogo de gato e rato dos filmes de Hollywood. O trabalho de segurança da informação era criar as políticas, treinar os colaboradores e auditar o cumprimento delas. Esses controles continuam sendo muito importantes, mas os maiores riscos estão migrando para as ameaças relacionadas a ataques cibernéticos e, com isso, um tipo diferente de profissional está ganhando espaço nas corporações, com conhecimentos sobre ataques e defesas cibernéticas e a missão de manter nossa organização dentre as que têm relação ruim de custo x benefício para o ataque, de forma que o atacante procure outro alvo, onde poderá lucrar o mesmo com muito menos esforço. É como uma manada correndo de um predador, os mais lentos ficarão para trás e serão devorados.

O cenário atual de ciberataques redefiniu as expectativas dos profissionais de segurança sobre o melhor cenário. Imaginar que possamos manter nossas empresas longe de ataques seria uma ingenuidade que pode custar caro. Precisamos tornar todos os controles apli-

cáveis para proteger nosso ambiente contra os ataques e, ao mesmo tempo, nos prepararmos para perder algumas batalhas, mas para sobrevivermos com nossos ativos mais preciosos intactos.

Se houve o tempo em que os dirigentes se perguntavam se seriam atacados, hoje a pergunta correta a fazer é quando e como seremos atacados e como reagiremos ao ataque. Praticamente não sobrou nenhum dispositivo IP que não possa ser utilizado para gerar dinheiro para os atacantes. Isso faz com que, a cada dia, descubramos um novo tipo de ataque, tendo como alvo tecnologias como câmeras IP, smartphones, smartTVs, roteadores wireless e qualquer outra "coisa" que se conecte à internet, também chamada de IoT (Internet of Things / Internet of "Trens", aqui em Minas).

## 1. Segurança da Informação x Cybersecurity

A segurança da informação compreende todas as disciplinas necessárias para manter a confidencialidade, integridade e disponibilidade das informações enquanto a segurança cibernética trabalha especificamente com os controles de segurança relacionados ao que acontece no ciberespaço, o espaço da internet. A cybersecurity trata de ações provocados por agentes humanos de ameaça, mas não trata de incidentes naturais, segurança física e erros pessoais dos usuários.

## 2. Red team x blue team – lições dos militares para a guerra cibernética

Em 1932, o general americano Harry Ervin Yarnell demonstrou, por meio de jogos de guerra, que Pearl Harbor era vulnerável a um ataque aéreo naval. Os responsáveis pela segurança da ilha não consideraram o ataque viável, concluindo o estudo com a seguinte observação:

> "É duvidoso que ataques aéreos possam ser lançados contra Oahu diante de uma forte aviação defensiva sem submeter os portadores atacantes ao perigo de danos materiais e, consequentemente, grandes perdas na força aérea de ataque".

Nove anos depois, Pearl Harbor foi atacada pelos novos caças "A6M Zero", desenvolvidos pela Mitsubishi para serem leves e rápidos, e fizeram exatamente o que a simulação de Yarnell previu: atacaram os aviões em solo, colocando os Estados Unidos na II Guerra Mundial.

Esses exercícios são até hoje uma das melhores técnicas utilizadas pelas forças armadas para aprimorar suas defesas e, inevitavelmente, foram adotadas para as batalhas mais importantes da atualidade: a guerra cibernética.

O profissional de segurança cibernética precisa analisar as políticas, tendências e informações da inteligência para entender melhor como os atacantes pensam e se comportam. Nesse intuito, as empresas formam internamente ou contratam times vermelhos (red team), que são os responsáveis por simular ataques à organização, utilizando os métodos que um atacante real utilizaria. A cada dia, o time vermelho tenta explorar uma nova vulnerabilidade ou a mesma de uma forma diferente. Não existe um limite para atuação do time vermelho, eles podem enviar spams, deixar um drive USB em uma área pública da empresa para que um colaborador infecte uma máquina ou ainda utilizar engenharia social por telefone e pela internet, explorando as redes sociais dos colaboradores da empresa. Impor limites ao time vermelho seria cometer o mesmo erro que os americanos cometeram em Pearl Harbor, julgar o limite inimigo pelos seus próprios limites.

Os times azuis (blue team) são os responsáveis por proteger a organização dos ataques do red team e dos ataques reais. Os times azuis se diferenciam das equipes de segurança da informação, pois não se envolvem em normas, redundância, segurança física e outras tarefas da equipe de S.I. O blue team possui mentalidade de vigilância constante contra o ataque, que, nos dias atuais, é uma realidade inevitável.

Obviamente, essa abordagem não é simples e requer diversos investimentos. A magnitude deles deve ser proporcional ao valor das informações a serem protegidas, mas sem que se subestime o potencial impacto financeiro e de imagem decorrente de um ataque que comprometa a confidencialidade, integridade ou disponibilidades desses dados. Quanto custará à Equifax o vazamento de 143 milhões de registros de cidadãos americanos e qual o impacto à Delloite, uma empresa de serviços e consultoria em cybersecurity, devido ao vazamento de e-mails com dados confidenciais de clientes em função de um cyberattack? Esse é o exercício que devemos fazer antes de postergar um projeto de proteção de dados, por meio da implementação de um framework de cybersecurity. As táticas utilizadas não deixam dúvidas de que estamos realmente em guerra, seja contra criminosos seja contra nações. Juntos, os times vermelhos e azuis aprimoram, diariamente, as defesas da organização, melhorando as técnicas de ataque e defesa.

## 3. Ferramentas para gestão da segurança cibernética

### ISO 27032 – Diretrizes para segurança cibernética

A ISO publicou em 2012 a norma ISO/IEC 27032, que trata da segurança do espaço cibernético, oferecendo

diretrizes para tratar os riscos de segurança cibernética mais comuns, incluindo:

- Ataques de âmbito coletivo;
- Hacking;
- Proliferação de softwares mal-intencionados ("malware");
- Softwares espiões ("spyware");
- Outros softwares potencialmente indesejados.

A diretriz técnica proporciona controles para lidar com esses riscos, incluindo controles para:

- Preparar-se contra ataques, por exemplo, de malwares, de meliantes particulares ou de organizações criminosas na internet;
- Detectar e monitorar ataques;
- Responder a ataques.

Para cumprir esse objetivo, a norma oferece os seguintes controles de segurança cibernética

- **Nível de aplicativo –** apresenta os controles que as aplicações web precisam oferecer para aumentar a segurança de seus usuários. Os controles vão desde as informações que devem ser passadas para os usuários até a revisão de código, prevenção de XSS, SQL injection e uso de HTTPS.
- **Proteção do servidor –** trata da segurança dos hosts que abrigam as aplicações que rodam no espaço cibernético e inclui gestão de atualizações (patches), antivírus e varreduras de vulnerabilidades (security scan).
- **Usuário final –** semelhante ao anterior, mas focado nas estações de usuários, inclui controles relacionados a bloqueador de script, filtro de phishing, firewall pessoal, etc.
- **Contra ataques pirataria cibernética (social engineering) –** trata da política de segurança, classificação da informação e sensibilização e formação dos colaboradores.
- **Prontidão da segurança cibernética –** aborda a detecção de eventos por meio do monitoramento da Darknet.

**NIST Cybersecurity Framework**

O National Institute of Standards and Technology (NIST), o equivalente à Associação Brasileira de Normas Técnicas (ABNT) nos Estados Unidos, desenvolveu o Framework for Improving Critical Infrastructure Cybersecurity, que está na versão 1.0, mas já com um draft público da versão 1.11.

O framework foi desenvolvido para gerenciar o risco de segurança cibernética e é composto por três partes: framework core, níveis de implementação do framework e perfis do framework.

- O framework core é um conjunto de atividades de segurança cibernética, resultados desejados e referências aplicáveis que são comuns em todos os setores de infraestrutura crítica. Consiste de cinco funções simultâneas e contínuas: identificar, proteger, detectar, responder e recuperar.
- Os níveis de implementação do framework ("tiers") tratam de como uma organização vê o risco de segurança cibernética e os processos para gerenciar esse risco. Os tiers caracterizam as práticas de uma organização em um intervalo, desde parcial (nível 1) até o adaptativo (nível 4). Esses níveis refletem uma progressão de respostas informais e reativas para abordagens ágeis e com risco de informação.
- Os perfis de framework podem ser usados para identificar oportunidades para melhorar a postura de segurança cibernética comparando um perfil "atual" (o estado "como está") com um perfil "alvo" (o estado "a ser").

**Figura 1 - Abordagem de cinco passos**

**Gartner Carta – Continuous Adaptive Risk and Trust Assessment**

A Carta é fruto da arquitetura de segurança adaptativa do Gartner e propõe uma abordagem continuamente adaptável à segurança da informação. O propósito da Carta é permitir que as empresas tomem decisões quando toda a informação não está disponível ou quando há um nível de risco conhecido, com base no risco e na confiança. Alguns dos principais conceitos da Carta incluem:

- As decisões devem se adaptar continuamente. As respostas de segurança devem se adaptar continuamente. O risco e a confiança devem se adaptar continuamente.

- Bloqueio inicial / permitir avaliações de segurança para acesso e proteção deixam as empresas expostas a ataques "Zero Day" e direcionados, roubo de credenciais e ameaças de elementos internos.

- A confiança e o risco devem ser dinâmicos, não estáticos e avaliados de forma contínua à medida que as interações ocorrem e o contexto adicional fica disponível.
- Os resultados de negócios digitais só podem ser otimizados quando a confiança digital é gerenciada de forma adaptável como um conjunto de medidas de confiança fino com atributos de risco e resposta multidimensionais.

De acordo com o Gartner, existem três fases de segurança de TI às quais a Carta pode ser aplicada – planejar (plan) / construir (build) / executar (run) .

- Na fase de planejamento e governança (plan), a Carta propõe uma forma mais dinâmica de se controlar o risco, avaliando constantemente e adaptando os controles. No geral, os analistas do Gartner disseram que a perfeição é inimiga do suficientemente bom, e as empresas precisam considerar controles adaptativos e avaliar continuamente os riscos para que não se tornem exageradamente conservadoras, utilizando decisões binárias sobre o que se pode ou não fazer.

- Essa mesma filosofia pode se estender ao mundo do desenvolvimento de aplicativos (build). À medida que as aplicações são construídas com blocos usando código aberto, é muito possível que existam vulnerabilidades nesses pacotes de software, e a Carta aparece alinhada com a disciplina de DevSecOps. Muitos aplicativos utilizam componentes de código aberto que contêm pelo menos uma vulnerabilidade significativa. O uso de tais pacotes pode tornar-se uma decisão baseada em risco, em vez de uma opção binária. A mesma abordagem pode ser usada ao analisar software e integrações de terceiros.

- No domínio da execução (run), o objetivo da Carta é otimizar o uso de recursos limitados para se concentrar nas maiores ameaças. A integração de análises ajuda a se concentrar em ameaças significativas ao mesmo tempo que automatiza a maioria dos incidentes. Uma vez que você reconhece que a prevenção perfeita é impossível, a resposta contínua torna-se uma realidade.

## 4. Preparação para cybersecurity

Segunda a Isaca, existem aproximadamente 410 a 510 mil profissionais de segurança da informação em todo o mundo, número que nem de longe cobre a demanda existente nas empresas. Para ocupar essas vagas, a tendência é que haja uma migração de profissionais de TI para segurança da informação e principalmente nas questões práticas de cybersecurity, uma vez que essa é mais focada nos aspectos técnicos da segurança.

Neste cenário, há uma procura crescente por profissionais com qualificação e certificações em disciplinas como Ethical Hacking, Investigação Forense, Desenvolvimento Seguro e Cybersecurity e uma oferta cada vez maior. Em um primeiro momento, a terceirização de serviços de segurança pode parecer a opção mais viável, mas as organizações precisam entender o que deve e o que não deve ser terceirizado. Uma operação de monitoração 24x7 é cara e, dependendo do porte da empresa, os profissionais podem ficar muito ociosos. Por outro lado, o planejamento e acompanhamento das métricas de segurança são mais eficientes à medida que o profissional de segurança da informação conhece a fundo os processos de negócio da empresa e se alinha com a governança e gestão da organização para evitar a parada desses processos ou a perda e vazamento de dados que podem tirar vantagem competitiva da organização.

O processo de aprendizado para lidar com essas questões estratégicas é longo e os valores em jogo são muito altos. Com certeza, conservar esses colaboradores e investir na qualificação deles para segurança é uma atitude sensata. A qualidade do time de profissionais de segurança da organização será mais relevante que todo o investimento feito em equipamentos de ponta adquiridos ou contratados para proteção dos dados. Um dispositivo de alto valor, mas mal configurado é quase inútil, enquanto um dispositivo construído com software livre ou gratuito pode ser extremamente eficaz se bem configurado e monitorado.

Como se vê, os profissionais de segurança e de TI fazem parte do conjunto de ativos de informação mais valiosos da empresa. Em última instância, as informações e pro-

cessos de negócio mais importantes das organizações estão nas mãos desses profissionais, e não somente no hardware ou software adquiridos.

Devido à escassez crescente de profissionais de segurança da informação capacitados, as organizações estão fazendo um movimento de preservar seus talentos e investir nessa movimentação de carreira. Para a gestão, é difícil avaliar se o profissional de segurança está ou não realizando um bom trabalho. A falta do conhecimento adequado sobre o assunto faz com que o próprio colaborador tenha uma falsa sensação de segurança, ele desconhece a real dimensão das ameaças e considera estar protegido. Associe isso ao *modus operandi* atual dos invasores e teremos um sistema invadido e completamente controlado por atacantes durante meses ou até mesmo anos, sem que o gestor tome conhecimento. O ideal é identificar os colaboradores com um perfil de aprendizado continuado e propor-lhes uma qualificação constante nas disciplinas de segurança da informação.

Diferentemente das doutrinas de TI, é necessária muita experiência para se certificar de que um programa de segurança da informação está sendo eficaz na proteção dos dados. Quando falamos de um estudo sobre servidores Windows, Linux, Virtualização ou qualquer outra disciplina técnica, um indicador de que o conhecimento foi absorvido é o próprio funcionamento adequado do sistema. Já na segurança da informação, uma organização pode fazer investimentos milionários e, mesmo assim, não obter o nível de segurança esperado, vivendo uma falsa sensação de segurança até o dia em que um incidente maior acontecer. Quando esse incidente ocorre, as empresas procuram uma auditoria externa, descobrem que seus sistemas de segurança tinham inúmeras falhas, mas não havia ninguém que entendesse o trabalho de segurança da informação a ponto de medir a qualidade do serviço do CSO (Chief Security Of ficer). Nesse ponto, resta à organização demitir o CSO, CIO e até mesmo o CEO, mas o estrago já está feito, e nada trará de volta a confiança na mesma.

Quando nos aprofundamos no estudo da segurança da informação, vemos que, dependendo do tamanho e do risco de uma organização, precisamos não apenas de um profissional bem treinado em segurança, mas de um time multidisciplinar criando políticas de segurança, arquitetando soluções técnicas, organizacionais, orientando e avaliando um processo de segurança de aplicações com desenvolvimento seguro e gestão de vulnerabilidades.

Tão vasto quanto o conhecimento necessário para a adequada proteção das organizações é o número de disciplinas a serem estudadas para manter um nível adequado de segurança, contando, na maioria das vezes, com especialistas em cada área da segurança da informação trabalhando em equipe. Para a formação de cada um desses profissionais, destacamos os seguintes programas de treinamento/certificação.

## 5. Segurança da informação (geral)

Se há um tempo o profissional de segurança da informação era um especialista que conhecia tudo sobre o assunto, hoje temos linhas de atuação bem distintas dentro da área. As primeiras certificações a serem abordadas são as mais generalistas, que analisam a segurança da informação de forma holística:

- **EXIN ISFS (Security Foundation) –** é o programa de certificação que serve como uma entrada no mundo da segurança da informação. Essa certificação não é apenas para os profissionais de segurança da informação, ela enriquece todos os profissionais de TI, que, por meio desse aprendizado, podem agregar valor às atividades do dia a dia. Nas palavras de Bill Gates, em 2002, quando lançou o programa de computação confiável da Microsoft: "Nós fizemos um ótimo trabalho até aqui, mas todos esses ótimos recursos não importarão, a menos que o consumidor confie em nosso software".

- **ISC2 CISSP –** na minha opinião, a certificação mais completa do mercado, que exige do profissional um conhecimento avançado de vários domínios, que vão de criptografia até continuidade de negócios e segurança física, passando por telecomunicações e desenvolvimento seguro e arquitetura de sistemas.

- **Isaca CISM –** trata-se de uma certificação para gestores de segurança, que foca no alinhamento com a governança e gestão da organização, além da criação de um programa de gestão da segurança da informação e de métricas para acompanhamento do desempenho do programa. Não espere por questões técnicas no CISM, mas, sim, por questões em que todas as opções levam ao resultado esperado, mas somente uma é a melhor forma de obter aquele resultado.

## 6. Cybersecurity

Esse tipo de certificação foca especificamente nas disciplinas relacionadas à proteção do espaço cibernético, elas abordam as disciplinas necessárias para o trabalho das equipes azuis e vermelhas.

- **EXIN Cyber & IT Security Foundation (Cisef) –** certificação bem técnica, voltada para profissionais de segurança, administradores de rede, desenvolvedores e auditores. Aborda temas como: redes TCP/IP, aplicações e bancos de dados, criptografia, gestão

de identidades e acesso, computação em nuvem e exploração de vulnerabilidades.

- **Isaca Cybersecurity Fundamentals –** essa é a primeira certificação técnica do Isaca e também a primeira do Programa Cybersecurity Nexus (CSX). O programa dessa certificação envolve os conceitos e princípios de arquitetura de cybersecurity, segurança em redes, sistemas, aplicações e dados, além de resposta a incidentes. Particularmente, acho essa certificação totalmente complementar à CISEF do EXIN, sendo que são duas certificações de entrada e com custo relativamente baixo.

- **Isaca CSX Practitioner –** um nível acima das certificações anteriores, a Practitioner trata das habilidades de resposta a incidentes, avaliando a capacidade de seguir processos definidos, trabalhar com problemas conhecidos dos sistemas, antivírus, firewall, atualizações (patching), além de realizar varreduras (scans) de vulnerabilidades e outras análises.

## 7. Desenvolvimento seguro

Um dos maiores vetores de ataque dos criminosos é a exploração de falhas de código. Um determinado sistema pode funcionar perfeitamente por vários anos, mas estar extremamente susceptível a explorações de vulnerabilidades. Os programadores foram treinados para escrever aplicações que respondessem a uma utilização correta, não foram preparados para prever ataques que subvertem o funcionamento da aplicação. O conhecimento em desenvolvimento será, em breve, condição essencial para qualquer desenvolvedor manter sua posição.

- **EXIN SPF (Secure Programming Foundation) –** é o primeiro nível de estudo para desenvolvedores, focando na conscientização e na compreensão das ameaças e medidas corretivas para evitar invasões aos sistemas. Assim como a Security Foundation, essa certificação agrega bastante a qualquer programador.

- **ISC2 CSSLP (Certified Secure Software Lifecycle Professional) –** assim como na CISSP, a ISC2 trabalha com conteúdo mais completo, tratando desde o design até a manutenção dos sistemas. Certamente uma excelente opção para os arquitetos de software.

## 8. Ethical Hacking

Se, de um lado, as organizações treinam os desenvolvedores para evitar as vulnerabilidades de código que podem levar a ataques de injeção de SQL XXS, entre outros, do outro lado do jogo, elas precisam formar seu Red Team, para testar a eficiência das aplicações e dos controles adicionais implementados pela área de TI e segurança. Para formar esse time, contamos com algumas certificações no mercado, das quais se destacam:

- **EXIN EHF (Ethical Hacking Foundation)** – certificação de entrada no mundo hacking, a EHF aborda as fases dos testes, os principais conceitos e as principais ferramentas para a análise e geração do relatório.

- **EC-Council CEH (Certified Ethical Hacking) –** certamente, a certificação mais famosa do EC-Council, a CEH é uma certificação mais completa, com muitos conceitos técnicos e uso de ferramentas para testes de invasão.

## 9. O caminho se faz caminhando

É muito importante levar sua empresa, de qualquer tamanho e orçamento, um (ou vários) passo(s) à frente das demais para que não se torne a próxima vítima. Os atacantes cibernéticos não são mais movidos somente a desafios, eles são objetivos e atacam as empresas menos preparadas para otimizar o tempo. Todo e qualquer investimento em segurança te colocará à frente de algumas outras empresas e dificultará a ação dos atacantes, mas o ideal é uma abordagem sistematizada, cobrindo todos os controles da segurança da informação.

Existem várias abordagens para se implementar a segurança cibernética em uma organização, dentre elas destacamos:

- **Ad hoc –** implantação de controles sem uma análise prévia de riscos e de prioridades, geralmente impulsionados por uma apresentação de fornecedor. Nesse ambiente, é comum encontrar equipes de TI que, não por falta de conhecimento ou engajamento, não exploram o potencial das ferramentas adquiridas, subutilizando-as e gerando enorme desperdício de dinheiro, uma vez que a segurança não é alcançada.

- **Baseada em conformidade –** focada somente em implantar os controles necessários para atender determinada norma, lei ou regulamentação. Esse modelo também se mostra muito frágil, pois fica evidente que não há comprometimento com a segurança em si, apenas em evitar as penalidades impostas por uma entidade no caso de uma auditoria negativa. Costumo dizer que chegar à conformidade sai caro, mas, com um pouquinho mais de esforço, se obtém segurança. A segurança real, baseada em riscos, tem relação custo x benefício muito mais positiva.

- **Baseada em riscos –** nessa abordagem, os riscos são identificados individualmente e classificados, para que se possa estabelecer um programa de redução, atuando na probabilidade ou no impacto de cada risco. Essa abordagem está normalmente baseada em controles descritos na ISO 27002 e acompanhada de varreduras de vulnerabilidades e testes de invasão, para aferir a real situação da empresa em relação à segurança.

Considerando todos os itens abordados neste artigo, entendemos que as maiores ferramentas para defesa cibernética são metodologias e conhecimento, o que coloca o fator humano em destaque na gestão da segurança da informação. É preciso criar processos, realizar análises frequentes de risco, treinar as equipes e colaboradores e utilizar tecnologias que apoiem esses processos, como SIEM (Security Information and Event Management), FIM (File Integrity Monitoring), Endpoint security, Firewall, IPS/IDS e outros. Enquanto a plenitude da inteligência artificial não é alcançada, são as pessoas que orquestrarão todos esses componentes.

**Referências**


**Gartner Group, How the Internet of Things Is Changing Cybersecurity**. Disponível em: http://www.gartner.com/smarterwithgartner/how-the-internet-of-things-is-changing-cybersecurity/. Acessado em: 2 out. 2017.

**Red team versus blue team: How to run an effective simulation**. Disponível em: https://www.csoonline.com/article/2122440/disaster-recovery/emergency-preparedness-red-team-versus-blue-team-how-to-run-an-effective-simulation.html. Acessado em: 2 out. 2017.

**CARTA - The Evolution of IT Security Beyond Black and White**. Disponível em: https://blog.preempt.com/carta-the-evolution-of-it-security-continuous-adaptive-risk-trust. Acessado em: 2 out. 2017.

# Como a cibersegurança chegou à era cognitiva: uma breve história

Arquivo pessoal


## João Paulo Lara Rocha

*Líder da unidade de negócios de Segurança da Informação da IBM Brasil. Atua há 17 anos no setor. Anteriormente, liderava na própria IBM as ofertas de gerenciamento de identidade e acesso na América Latina, apoiando as demandas de negócios e o cumprimento das regulações. Formado em Processamento de Dados pelo Centro Universitário Planalto do Distrito Federal (Cesubra), pós-graduado em Segurança de Redes de Computadores e mestrado em Gestão do Conhecimento e Tecnologia da Informação pela Universidade Católica de Brasília. Possui certificações CISSP e CISA.*



### Resumo

*Desde a Antiguidade, histórias ilustram como algumas guerras foram vencidas por meio de estratégias para romper barreiras que pareciam indestrutíveis. O lendário conto do Cavalo de Troia, criado pelos gregos por volta de VIII a.C., à Linha Maginot, na Europa, na Segunda Guerra Mundial, mostram que ataques que se aproveitaram da vulnerabilidade do oponente sempre existiram. Atualmente, essas batalhas são travadas no mundo digital, e o oponente, geralmente, é desconhecido e se camufla na mais profunda internet. Este é os cibercriminoso: um perigo real, e é preciso estar preparado para se proteger.*



***Palavras-chave:***
*segurança da informação, malware, vulnerabilidade, cibercriminosos.*


No princípio, tudo era escuridão. E, por diversos historiadores, assim era conhecida a Idade Média. O período medieval foi reconhecidamente uma época em que diversas pragas, sucessivas guerras e invasões bárbaras assolaram a civilização. Nesse mesmo período, estavam sendo formados novos reinados e existia uma demanda grande para proteger não só as pessoas que viviam naquele local, mas também os seus bens mais valiosos, como as joias da coroa.

Um dos métodos mais eficazes para se defender dos ataques bárbaros, cavaleiros de outros reinos ou mesmo de saqueadores que viviam nas proximidades era edificando castelos. Isso porque, além de isolar fisicamente o terreno por meio da construção de fossos e de servir como forma de abrigo à população, também era uma forma de criar torres que proporcionavam pontos elevados de vigilância no local – o que garantia uma vantagem estratégica, permitindo um prazo melhor de preparação contra os ataques, sendo possível antecipar-se às ameaças antes mesmo que elas chegassem ao perímetro físico do castelo.

Essa técnica de defesa mostrou-se eficaz durante vários anos, permitindo que civilizações pudessem se estabelecer, crescer e prosperar. Porém, um episódio específico ficou marcado em todos os livros de história que relatam a mitologia grega: a guerra de Troia. Nessa batalha, o fator que mudou todos os fatos foi uma ação dissimulada de Odisseu, que, ao fingir que os gregos haviam desistido da guerra, deixou na praia um grande cavalo de madeira e bateu em retirada com os próprios navios. Os troianos, sentindo-se orgulhosos pela derrota dos inimigos, decidiram levar esse grande cavalo de madeira para o interior de sua cidade, como símbolo de sua vitória.

Somente umas aspas aqui para acompanhar essa narrativa, Sun Tzu, conhecido general, filósofo e estrategista chinês, tinha uma frase que se aplica muito bem a esse caso: "Diante de uma larga frente de batalha, procure o ponto mais fraco e, ali, ataque com toda a sua maior força". E isso foi exatamente o que aconteceu em Troia: um cavalo de madeira oco, repleto de soldados, que penetrou as fortalezas da cidade trazido pelos próprios troianos, foi o elemento perfeito para adentrar o ponto mais fraco das defesas (uma estratégia de ataque nova, sem precedentes), e esses soldados foram capazes de desferir um ataque letal a Troia, que, por fim, pereceu em chamas.

Há um ditado popular que fala que a história sempre se repete, e não poderíamos deixar de constatar esse fato

também em batalhas épicas, como o ocorrido na Segunda Grande Guerra. Muitos livros históricos revelam como algumas fronteiras podem ser transponíveis. Os franceses, com receio de serem atacados por terra pelo exército alemão, construíram um sistema de defesa ao longo da fronteira alemã. Essa demarcação à época ficou conhecida por "Linha Maginot", em homenagem ao veterano de guerra e ministro francês André Maginot.

Contudo, devido a erros estratégicos, tempo e orçamento, essa linha não se estendeu até o Mar do Norte e, por consequência, fez com que essa barreira se tornasse totalmente inútil em seu propósito inicial, uma vez que os alemães acabaram por invadir a França pela fronteira franco-belga, onde não havia sido construída a tal Linha Maginot.

Meu pai, apropriando-se da sabedoria popular, sempre me dizia que o rio achava um jeito de chegar ao mar, pois havia aprendido a encontrar um novo curso ao encontrar um obstáculo.

Mas o que tudo isso tem a ver com as ciberameaças? Simplesmente tudo! Esse referencial nos ajudará a ver como a segurança da informação evoluiu, principalmente no que tange ao espaço ciber. Até pouco tempo atrás, os mundos físicos e virtuais (ciber) eram separados e sem nenhuma conectividade ou correlação entre eles. Porém, isso já não é mais assim. Sabemos que uma ameaça virtual pode impactar a vida de pessoas e que praticamente não existe mais diferença entre o que é físico ou o que é virtual.

A medicina moderna é um dos exemplos dessa mescla. Por exemplo, atualmente, já é possível comandar remotamente a aplicação de insulina em um paciente por meio de um dispositivo implantado em seu corpo e que, conectado à internet, envia as taxas de glicose para um computador central que monitora a saúde desse indivíduo. Outro exemplo de que a internet das coisas, ou, em inglês, Internet of Things – IoT, está impactando de forma positiva nosso dia a dia são os sensores espalhados nos campos de colheita, que permitem o uso inteligente de água para irrigação do solo e são conectados a sistemas meteorológicos, que possuem análise preditiva que verifica se existirá ou não possibilidade de chuva para que o local seja ou não irrigado.

Entretanto, nem todos os exemplos são positivos. Como muitos sabem, estamos passando por uma grande transformação digital. A evolução tecnológica tomou conta das vidas das empresas e pessoas e a digitalização de serviços permitiu que estivéssemos, cada vez mais, conectados. Veja-se por exemplo, nossa interação com o mundo virtual. Hoje, grandes volumes de transações financeiras são realizadas por meio de serviços como internet banking, compras de passagens aéreas ou de bens de consumo no varejo em geral. Como manipulamos essas transações? Por meio de diversos dispositivos, sejam eles móveis, como celular, notebook, tablet, etc., sejam fixos, como computador.

Para termos a ideia de como o mundo mudou nos últimos anos, a internet comercial no Brasil completou 20 anos em 2015, e hoje já possuímos mais de 100 milhões de internautas brasileiros. Se olharmos então o número de smartphones no Brasil, mercado com pouco mais de 10 anos de existência, já vai chegar ao final do ano de 2017 com uma média assustadora de um smartphone por habitante (aproximadamente 208 milhões de smartphones), segundo estudo da Fundação Getúlio Vargas de São Paulo (FGV-SP).

Também podemos ver essa mudança no comportamento dos usuários bancários. Pesquisa recente da Federação Brasileira de Bancos (Febraban), publicada em 2017, mostra uma consolidação dos canais digitais – pela primeira vez, o mobile superou a internet. Se somarmos apenas o volume de transações dos canais digitais (mobile e internet), chegamos à impressionante quantia de 36,7 bilhões de transações, o que representa 57% do total das operações realizadas em 2016, ano base da pesquisa.

Outro ponto destacado na análise é que a confiança do consumidor nos canais digitais é reforçada pela segurança e praticidade oferecidas pela tecnologia, aliadas ao crescente acesso da população brasileira à internet e aos smartphones.

Contudo, não tocamos com frequência na segurança dessas operações que são feitas por meio desses equipamentos conectados à rede. Veja bem, se existe alguma forma de moeda envolvida nessas transações, seja dinheiro real ou o virtual, infelizmente também existem pessoas (ou organizações) que ocupam o seu tempo em descobrir como se beneficiar de falhas de sistemas para proveito próprio. Surgem então os criminosos virtuais, ou, mais conhecidamente, cibercriminosos.

Em outras palavras, os canais digitais tornaram-se convenientes para o uso dos clientes. E essa conveniência leva ao aumento natural de seu consumo. Você se lembra da última vez que foi a uma agência bancária? De ter que passar em um detector de metais antes de poder adentrar ao espaço onde estão os caixas? Com todos os incidentes que tivemos em agências bancárias, existe hoje uma proteção adequada e que coíbe a ação dos criminosos. Essa mesma maturidade existe no mundo ciber? Assim como o rio encontra o mar, independentemente das dificuldades que encontra pelo caminho, percebemos os criminosos migrarem para o meio vir-

tual, a fim de encontrarem um espaço mais atrativo e, em teoria, com menor chance de serem presos ou de entrarem em confronto com a polícia, como víamos em assaltos a bancos.

Mas quão atrativo é esse mercado? Como saímos dessa escuridão em que não existiam computadores e, em menos de um quarto de século, a internet deixou de ser ficção científica para se tornar uma realidade que utilizamos a cada momento? Os invasores bárbaros buscavam o ouro, as joias da coroa, já esses novos invasores (cibercriminosos) buscam, além dos benefícios financeiros, o ativo mais importante das companhias: seus dados corporativos e de seus clientes. E o que são os dados senão o que temos de mais importante, não é? Embora não seja a mesma definição, vou simplificar essa explicação utilizando a palavra informação. Por exemplo, quanto custam as informações sobre o comportamento de determinado consumidor, o número de cartão de crédito e documento de identificação? São tantas inserções diárias de todos os tipos que isso vira um banquete dos deuses para qualquer invasor.

Antes de falarmos da proteção do espaço ciber, vejamos primeiramente como evoluiu a área de tecnologia da informação, principalmente quanto à oferta de serviços e como chegamos a esses canais digitais que consumimos atualmente.

Voltando à década de 80, a maioria dos computadores aos quais tínhamos acesso eram os conhecidos "terminais burros", que eram computadores com (quase) nenhuma capacidade de processamento e armazenamento, que dependiam de conectar-se a um computador central, com maior capacidade de processamento, para realizar alguma tarefa.

Esses computadores centrais continham todos os dados e somente pessoas com alta especialização e treinamentos conseguiam operá-los. Eram bastante complexos, pois o acesso era bem restrito e da mesma forma também era a capacidade de processamento. Na verdade, a cada 18 meses, crescia em 100% essa habilidade de computação da máquina, enquanto o custo de fabricação permanecia o mesmo, segundo a Lei de Moore. Ainda que essa lei não seja capaz de se perpetuar por muito mais tempo, ela tem se mantido verdadeira até os dias atuais. E eu acho incrível pensar que, hoje em dia, temos em nossas mãos smartphones que possuem uma capacidade computacional maior do que tinha, na época, o computador da Nasa que levou o homem à lua.

Com a redução dos custos e o aumento da quantidade de processamento, armazenamento e também de computadores, as organizações começaram a aumentar a gama de serviços e aplicações que eram disponibilizadas por meio de redes, além de também distribuírem isso em diversos computadores geograficamente espalhados, conforme a necessidade do negócio. Com isso, não havia mais como manter o mesmo controle de acesso que os terminais burros e a segurança da informação se via diante de um novo problema: como controlar o acesso a tantos computadores?

Criar uma rede de computadores que ficasse dentro de um perímetro onde os dados e serviços ficassem protegidos e contidos, por meio de barreiras, e que somente aos acessos autorizados (válidos) deveria ser permitida a entrada (lembram-se dos castelos?), seria essa a solução adotada: a criação de ambientes logicamente segregados. Uma vez mais estamos aplicando na segurança da informação uma técnica derivada de um conceito militar. A aplicação mais atual desse conceito é uma faixa de terra para contenção militar em terreno praticamente hostil, chamada zona desmilitarizada, ou DMZ (do inglês demilitarized zone), que existe entre as fronteiras da Coreia do Sul e da Coreia do Norte, com 4 km de largura e 238 km de comprimento, cuja função é proteger o limite territorial de tréguas entre as repúblicas coreanas.

Voltando ao ambiente ciber, as empresas colocam os seus servidores (e por consequência os dados) em uma ou mais DMZs para que os serviços (ou aplicações) possam ser disponibilizados para serem acessados por pessoas (ou outros serviços ou dispositivos) pela internet. Esse controle de acesso é feito por meio de um elemento de rede com a função de bastião, conectado entre o segmento de rede em que é possível ter o controle (confiável) e um ambiente na internet (hostil), por exemplo. A esse bastião denominamos firewall, que foi batizado por possuir o mesmo princípio de uma porta de incêndio tradicional, cuja função é a contenção do incêndio.

Mas então colocar firewalls na rede me permite estar em um ambiente seguro? Já aprendemos com a Linha de Maginot que termos apenas uma barreira de defesa não é o suficiente para estarmos protegidos. E não era mesmo. Pequenos programas de computador capazes de causar lentidão, roubar dados e até tomar controle de uma máquina começaram a ser desenvolvidos por cibercriminosos. Esses programas foram batizados de vírus por serem capazes de trazer uma "doença" ao computador, mas, atualmente, por terem evoluído a outros tipos de ameaças, são chamados, de forma geral, malwares – termo em inglês cunhado para categorizar esses tipos de programas de computador que, muitas vezes, atuam como pragas virtuais.

Um tipo de malware bastante conhecido é o que se passa de forma despercebida, que dificilmente é detectado pelas defesas de perímetro de uma corporação e também pelo antivírus do computador do usuário, no qual se instala e começa a causar danos não só ao computa-

dor infectado, mas também aos demais computadores que possuem conexão pela rede. Adivinhem o nome que se dá a esse tipo de malware? Cavalo de Troia! Não à toa foi denominado dessa forma, não é mesmo?

No ambiente de tecnologia da informação, possuímos diferentes tipos de modelos e marcas de computadores, sejam estações de servidores, sejam de trabalho; vários sabores de sistemas operacionais, tipos e arquiteturas de servidores web, aplicação e de banco de dados, o que, por muitas vezes, nos dá a liberdade de escolha da melhor arquitetura e a mais conveniente para a empresa nos aspectos de custo e benefício. Porém, existe outro lado da moeda: isso também causa uma grande complexidade do ambiente para a manutenção e proteção contra ameaças. Entenda que quando se descobre uma falha de sistema (vulnerabilidade) – que pode causar danos como roubo, acessos indevidos ou simples indisponibilidade do acesso aos dados –, o fabricante do software disponibiliza uma versão de correção, mais conhecida como patch ou fix.

Aplicar uma correção ou atualização de sistema, na maioria das vezes, não é uma tarefa das mais complexas. A complexidade é conseguir, nos dias atuais, realizar uma parada programada nos serviços e garantir que, depois da atualização, não haja impacto na prestação dos serviços. A maioria das empresas trabalha com Acordos de Nível de Serviço (ANS ou do inglês Service Level Agreement, SLA), que preveem a indisponibilidade de apenas minutos ou poucas horas por ano e com multas pesadas em caso de descumprimento dos SLAs.

Além disso, ainda existe a possibilidade de que o fabricante (ou desenvolvedor do software) não exista mais ou a versão do sistema em uso se torne obsoleta, para a qual o fabricante já avisa que não dará mais suporte a tal versão. Felizmente, existem soluções capazes de aplicar as correções de forma automatizada, de acordo com regras de negócio ou ainda aplicar um patch virtual, fazendo uma correção paliativa até que uma próxima janela de mudanças esteja disponível.

Todas essas ferramentas de segurança para manter a infraestrutura de TI funcional geram alertas das formas mais variadas, que são somados aos inúmeros registros (logs) que são gerados por elementos de conectividade, aplicações, servidores web e demais componentes que fazem parte do parque tecnológico de uma empresa. E, com o aumento do consumo de serviços digitais, também aumenta, na mesma proporção, a quantidade desses logs e, por consequência, a complexidade de monitoração e detecção de ameaças.

Assim como a área de negócios de uma empresa lança mão de ferramentas de Business Intelligence para poder entender o comportamento de compras dos clientes, suas demandas e também otimizar o processo de vendas para gerar maior resultado, a área de segurança da informação precisou criar soluções analíticas e de inteligência para lidar com esse volume absurdo de eventos de segurança.

Deparamo-nos então com uma nova geração de ferramentas de cibersegurança, que começam a atuar no tripé: monitoria, detecção e resposta a incidentes. Elas se mostraram eficazes por um bom tempo, pois se colocavam em um patamar em que era possível automatizar ações por meio de eventos já conhecidos ou regras de negócio corriqueiras, tais como: "se o usuário acessou o correio eletrônico e está de férias, alerte"; "se o disco do servidor está ficando cheio, faça uma limpeza dos dados antes que fique sem espaço em disco"; "se um computador está com o antivírus desatualizado, aplique a versão mais nova da vacina" e assim por diante.

O problema que acabou acontecendo é que o atacante descobriu como burlar esses sistemas automatizados e começou a fazer ataques mais elaborados, com poucas chances de ser detectado e cada vez mais silenciosos, tornando a sua detecção cada vez mais complexa. Em seu último estudo sobre o custo de vazamento de dados, o Ponemon Institute revela que, em média, um ataque atualmente demora 270 dias para ser detectado. Inclusive, esse mesmo levantamento aponta que quanto mais tempo as companhias demoram para identificar um ataque e contê-lo, maior o custo para reparar os dados que forem roubados. Voltando aos ataques elaborados de hoje em dia, eles são chamados Advanced Persistent Threats – ou ameaças avançadas persistentes. O termo persistente se dá principalmente pelo fato de que o atacante quer manter-se dentro de uma corporação por mais tempo possível sem ser detectado, causando danos de forma contínua.

A maioria dos ataques hoje acontece também devido a descobertas de vulnerabilidades chamadas de dia zero. Ou seja, essas fragilidades são exploradas muitas vezes por esses criminosos que buscam burlar sistemas – e que não podem ser detectadas ou correlacionadas pelos sistemas de detecção, pois simplesmente é a primeira vez que elas ocorrem e nenhuma regra ainda havia sido criada para detectá-las. Isso faz com que as defesas demorem a responder ao incidente e, em muitas vezes, o dano já foi causado.

Uma das formas que tem sido utilizada para reduzir esse tempo de detecção de um ataque é o investimento no comportamento da rede e de seus usuários, para que, de uma forma analítica, seja possível detectar um comportamento anômalo e alertar quanto a uma possível mudança de comportamento que indique um ataque em andamento. A tal capacidade chamamos de User Behaviour Analytics ou User and Entity Behaviour

Analytics, se estivermos também captando dados analíticos de outras entidades que não só os usuários.

Entretanto, como é possível dizer que uma atividade é anômala ou não? Como entender o comportamento de uma rede cada vez mais complexa? Atualmente, o número de conexões que um único computador faz na internet é enorme, ainda mais com a quantidade de serviços disponibilizados na tão famosa nuvem computacional que cresce a cada dia mais e mais. Um analista de negócios mais um especialista em segurança da informação poderiam dizer se é realmente uma anomalia ou foi apenas um falso positivo gerado pela ferramenta de monitoração?

Na maioria das vezes, o volume de eventos a ser monitorado é tão absurdo que fica difícil de acompanhar. Na verdade, isso me faz lembrar o filme *Matrix*, no qual há uma cena em que os operadores conseguem decifrar milhares de caracteres que passam em uma tela verde e "traduzem" tudo o que está passando no momento e, em tempo real, alertam: ali há uma falha no sistema! Que coisa mais insana, não é mesmo?

Poderíamos então investir na contratação desses operadores ou mesmo em analistas altamente capacitados que vão atuar contra esses cibercriminosos e ter um batalhão de profissionais de segurança da informação prontos para erradicar essas ameaças. Porém, infelizmente, não parece ser essa a resposta. Uma previsão recente da Gartner, consultoria de tecnologia da informação e comunicação (TIC), aponta que, até 2020, teremos, globalmente, uma escassez de 1,5 milhão de profissionais de segurança da informação.

Vamos pensar: está comprovado que as ameaças aumentam exponencialmente. Ataques recentes, como o WannaCry e o Petya, causaram indisponibilidade em serviços de várias corporações em todo o mundo. A esse novo tipo de malware que causa o embaralhamento (criptografia) dos dados de um computador, fazendo com que a pessoa que foi afetada tenha que pagar um valor, muitas vezes em moeda virtual, para poder reaver seus dados, como se fosse um sequestro virtual, se dá o nome de ransomware.

Se temos hoje ataques avançados, ferramentas de segurança e ambientes complexos para gestão e ainda escassez de profissionais, podemos então pensar que estamos perdendo essa guerra? Para a nossa tranquilidade, a resposta é não. E isso é incrível!

Vamos lá! Assim como nos castelos medievais, a vigilância das torres poderia detectar ameaças antes mesmo de elas chegarem aos perímetros do castelo, adicionamos ao tripé detecção, monitoramento e resposta a incidentes outro elemento importantíssimo: o cyber threat intelligence.

No cenário de segurança, a análise de dados se torna mais do que necessidade, se pensarmos no grande volume de informações diagnosticada chegando aos sistemas de segurança a cada minuto. De forma simplificada, o que se espera é a obtenção de informações a partir de fontes dispersas pelo ciberespaço. Essas fontes seriam como sensores de longo alcance que avisariam sobre incidentes que estão acontecendo em outros lugares, bem antes de chegarem ao ambiente de uma empresa, como se fosse um sistema de alerta de tempestades ou furacões. A partir desses avisos externos e colocando dentro do contexto da organização, é possível antever e tomar uma decisão com muito mais precisão de como mitigar ou prevenir um ataque.

Várias empresas de segurança da informação e blogs especializados realizam esses alertas, algumas vezes pagos, outras vezes de forma gratuita. A complexidade aqui está em decidir quais fontes de inteligência são confiáveis e quais se aplicam ao próprio negócio. Hoje em dia, por meio de ferramentas de segurança, é possível compartilhar inteligência contra ameaças digitais com tanta rapidez e eficiência quanto as que os invasores conseguem impor.

Em um mundo globalizado, temos visto cada vez mais que os alertas não têm hora para chegar, pois podem vir de um evento que aconteceu do outro lado do mundo, enquanto todos no Brasil estavam dormindo e vice-versa. Precisaríamos, então, de uma pessoa ou inteligência que fosse capaz de receber informações em tempo real de blogs, fabricantes diversos, estarmos atentos a conversas na deep web sobre possíveis ataques novos e ainda não esquecermos de tudo o que já lemos. Para ter uma ideia sobre essa internet mais obscura, temos uma infinidade de dados. Contudo, de todos os disponíveis conseguimos somente visualizar 20% a partir de pesquisas básicas. Em linhas simplificadas, imagine uma pedra na margem de um rio. Parte está dentro da água e parte fora. O que vemos? O que dizemos é que os 80% restantes estão embaixo da água. Traduzindo, hoje temos a deep web – onde encontramos informações acadêmicas, documentos legais, relatórios científicos e registros, entre outros – e a dark web – com informações ilegais, comunicações privadas, tráfico de drogas e armas, etc.

Com todo esse cenário, imagine se toda a função de rastrear e estar atenta a esses dados fosse realizada por uma só pessoa. Olha, não direi que seria impossível, mas seria bastante difícil e custoso mantermos uma equipe com tamanha especialização devido à carência de profissionais que possuímos. E aqui é o ponto a que eu quero chegar com este artigo: ter a nosso favor a inteligência cognitiva!

Com base na nuvem, a inteligência cognitiva hoje é capaz de consumir todas as informações já produzidas e as

novas que são geradas diariamente sobre o domínio de conhecimento de segurança da informação e começar a prover insights sobre o que está acontecendo neste exato momento, dando ainda contexto com os eventos que estão sendo gerados dentro da sua corporação.

Só para esclarecer um pouco, a inteligência artificial é a área da ciência da computação que tenta recriar a inteligência humana em máquinas. Hoje entendemos que ela é considerada como a terceira era computacional. O aprendizado dessa tecnologia é feito em larga escala e ela "raciocina" de acordo com propósitos, cria hipóteses e interage com os humanos de forma natural, ou seja, como um ser humano falando com o outro. Sempre utilizo uma ilustração bem bacana para mostrar como a inteligência artificial funciona. Pensemos em uma pesquisa básica no famoso buscador da atualidade, o Google. Se digitarmos a seguinte frase na barra de busca: "Quero ver todos os alimentos exceto bananas". O que a ferramenta irá mostrar? Bananas! Na inteligência artificial, ela consegue te dar exatamente o que procura e, se tiver interesse, poderá, inclusive, receber informações mais aprofundadas sobre determinadas hortaliças, por exemplo.

Nos dias atuais, a inteligência cognitiva já faz parte da realidade de organizações do mundo inteiro e também aqui no Brasil. Graças a ela, os profissionais de segurança da informação podem agora contar com um aliado que lhes permite resolver problemas de segurança não em dias, mas, sim, em minutos. Isso porque essa tecnologia gera insights que auxiliam no descobrimento de grande parte das intenções de ataques aos tais dados submersos. Por meio do raciocínio e aprendizagem dos dados não estruturados que mencionei anteriormente, essas plataformas conseguem oferecer cognição de segurança em larga escala.

É importante também desmistificar que a máquina substituirá o homem. Na verdade, a intenção não é a de colocar ninguém no lugar de ninguém, mas sim de permitir que um analista possa, por meio dos insights, resolver de forma mais rápida os incidentes de segurança e ainda poder orquestrar todas as respostas aos incidentes de forma automatizada. Ou seja, o papel principal da inteligência artificial nesse sentido seria o de aumentar a capacidade cognitiva do profissional, dando insumos para melhor tomada de decisão.

Assim como um farol que ilumina a navegação noturna, a inteligência cognitiva veio para trazer luz à disciplina de cibersegurança, permitindo que usuários possam desfrutar de serviços digitais com confiança e possibilitando vida longa, próspera e segura ao mundo ciber.

**Referências**


FGV. http://eaesp.fgvsp.br/sites/eaesp.fgvsp.br/files/pesti2017gvciappt.pdf. Acessado em: 2 out. 2017.

FEBRABAN. https://cmsportal.febraban.org.br/Arquivos/documentos/PDF/Pesquisa%20FEBRABAN%20de%20Tecnologia%20Banc%C3%A1ria%202017.pdf. Acessado em: 2 out. 2017.

FROST & SULLIVAN. https://iamcybersafe.org/wp-content/uploads/2017/06/Europe-GISWS-Report.pdf. Acessado em: 2 out. 2017.

# Cibersecurity: o foco da proteção é só tecnológico?

Arquivo pessoal


## *Márcio Antônio da Rocha*

*Vice-presidente de Governança, Riscos e Compliance (GRC) da Sucesu MG, sócio-diretor da Aéras – Segurança da Informação, membro da OCEG e do CB21 – SC02 – ABNT, consultor especializado em GRC e Segurança da Informação. Trabalha na área de TI há 46 anos, em diversas empresas no Brasil e no exterior. Possui larga experiência, nacional e internacional, em gestão de negócios, gestão de projetos de tecnologia e de segurança da informação, segurança da informação e gestão da continuidade de negócio. Há 16 anos trabalha como consultor em Segurança da Informação, GCN e GRC. Membro da comissão CEE-63 (Estudo Especial de Gestão de Riscos) da ABNT (Associação Brasileira de Normas Técnicas) e membro do Conselho Diretor Executivo da Sucesu MG, desde 2003.*



### *Resumo*

*Este artigo tem o objetivo de abordar a guerra cibernética, o desafio enfrentado pelas empresas e o que efetivamente elas estão ou deveriam estar fazendo para combatê-la. Pretende contribuir para que o leitor considere como fator primordial o alinhamento das iniciativas de segurança com os riscos do negócio e por meio da adoção de um método que permita que a organização possa medir a maturidade das disciplinas de segurança e determinar a maturidade da segurança organizacional. Mostra que, embora o cenário seja complexo e assustador, existe um farto material de apoio para orientar os profissionais e executivos na tarefa de tornar o ambiente empresarial mais seguro, mantendo o cerne nos processos críticos de negócio, e apresenta alguns pontos fundamentais para um modelo de Governança de Segurança Organizacional.*



***Palavras-chave:***
*espaço cibernético, segurança cibernética, proteção, segurança da informação, guerra cibernética, defesa cibernética, 4ª revolução, tecnologia, governança.*


## 1. Contextualização

> "Estamos à beira de uma revolução tecnológica que alterará, fundamentalmente, a forma como vivemos, trabalhamos e nos relacionamos um com o outro. Em sua escala, alcance e complexidade, a transformação será diferente da que a humanidade já experimentou. Ainda não sabemos como isso vai se desenrolar, mas uma coisa é clara: a resposta a ela deve ser integrada e abrangente, envolvendo todas as partes interessadas da política global, dos setores público e privado ao meio acadêmico e à sociedade civil." (Klaus Schwab)

Considerando esse contexto, assegurar a proteção das informações adotando medidas que garantam um nível aceitável de segurança da informação ganha grande importância nas decisões estratégicas da organização. Buscar uma maior qualidade dos serviços e a proteção adequada das informações torna-se uma atividade prioritária dos executivos do negócio diante da adoção das novas tecnologias.

No contexto da 4ª Revolução[1], a defesa cibernética[2] passa por um momento instigante e fascinante. Crescem os incidentes de segurança de perdas maciças de dados, o roubo de informações, o roubo de propriedade intelectual, as violações de cartão de crédito, o roubo de identidade, as ameaças à nossa privacidade, negação de serviço, e as organizações estão enfrentando uma grande pressão para garantir que os seus dados estejam seguros. Este é o modo de vida para todos nós no ciberespaço.

***ISTR, Ransomware 2017, An ISTR Special Report, Analyst: Dick O'Brien - SYMANTEC***

*Durante os primeiros seis meses de 2017, as organizações contabilizaram um total de 42% das infecções por ransomware[1], acima dos 30% em 2016 e 29% em 2015. Essa mudança foi principalmente representada por WannaCry e Petya.*

*[1]Ransomware é um tipo de código malicioso que torna inacessíveis os dados armazenados em um equipamento, geralmente usando criptografia, e que exige pagamento de resgate (ransom) para restabelecer o acesso ao usuário. (Cartilha de Segurança – Ransomware, https://cartilha.cert.br/ransomware/).*

Em contrapartida, os defensores têm acesso a uma extraordinária variedade de conhecimento teórico e prático sobre os domínios da segurança da informação e GRC[3], normas, padrões e frameworks de segurança, grande oferta de treinamento e certificações, aplicações de gerenciamento e monitoramento de segurança e tecnologia, bases de dados de vulnerabilidade, catálogos de controles de segurança, inúmeras listas de verificação de segurança, etc. Mais ainda, há informações que ajudam no entendimento de ameaças por meio do conhecimento compartilhado, interno e externo de ameaças, como feeds, relatórios, ferramentas, serviços de alerta que contribuem para facilitar a compreensão sobre as ameaças, além dos requisitos de segurança, estruturas de gestão de risco e conformidade, exigências regulatórias e muito mais. Não há escassez de informações disponíveis para ajudar os profissionais de segurança sobre o que devem fazer para garantir a confiabilidade, integridade e disponibilidade de sua infraestrutura tecnológica que suportam a operação dos negócios.

## 2. Introdução

Este artigo discute alguns dos complexos desafios enfrentados pelos profissionais responsáveis pela segurança do espaço cibernético e apresenta sugestões para enfrentá-los segundo a visão do negócio e não apenas a visão tecnológica. A Figura 1 abaixo ilustra a abrangência desse tema.

A aplicabilidade das mais diversas formas de tecnologia como recurso estratégico e fundamental nos processos de negócios, além de garantir a agilidade no trato das informações, é cada vez mais crescente a utilização da tecnologia como alternativa estratégica para a transformação dos negócios. Portanto, cada vez mais, é necessária a adoção de mecanismos e práticas que garantam a segurança dessas informações em todo o ciclo do processo do negócio. Conceitos de confidencialidade, integridade e disponibilidade devem ser considerados em qualquer processo de negócio da organização. A Figura 2 exemplifica esse contexto.

**Figura 1 – Adaptada a partir da relação entre a segurança cibernética e outros domínios de segurança descrita na norma ISO/IEC 27032:2015[4] - Tecnologia da Informação - Técnicas de Segurança - Diretrizes para Segurança Cibernética**

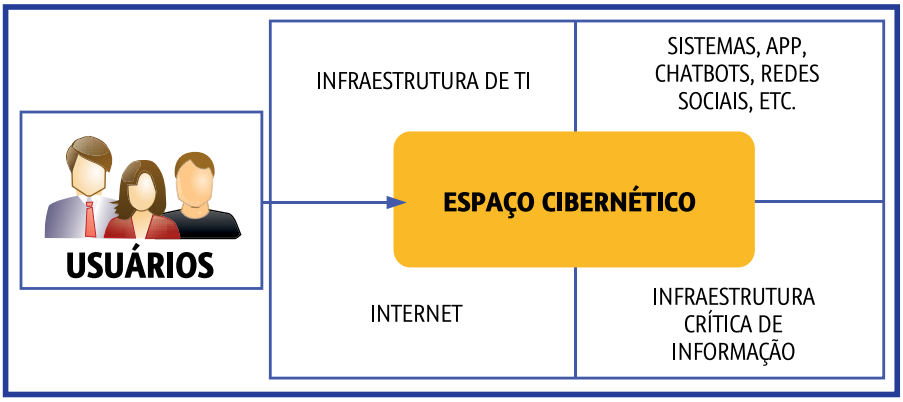
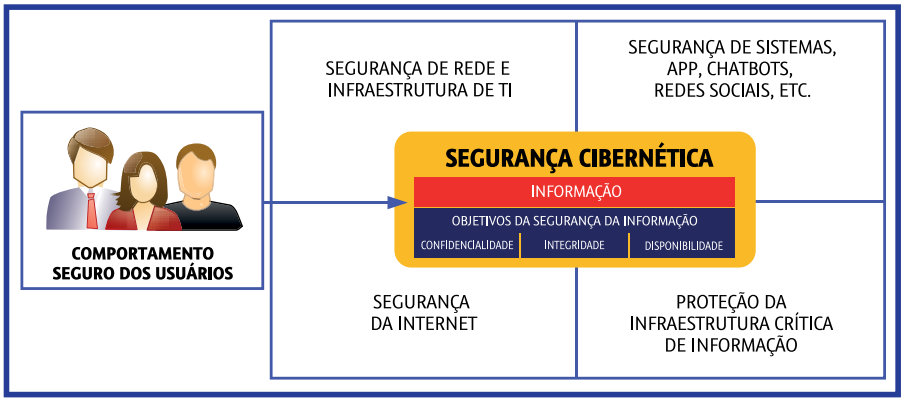



**Figura 2 – Adaptada a partir da relação entre a segurança cibernética e outros domínios de segurança descrita na norma ISO/IEC 27032:2012 - Tecnologia da Informação - Técnicas de Segurança - Diretrizes para Segurança Cibernética**




1 https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond , Klaus Schwab. Acessado em: out. 2017.
2 Center for Internet Security (CIS) Critical Security Controls for Effective Cyber Defense (CSC): https://www.cisecurity.org. Acessado em: out. 2017.
3 GRC – Governança, Riscos e Compliance.
4 Esta Norma fornece diretrizes para melhorar o estado de segurança cibernética, traçando os aspectos típicos dessa atividade e suas ramificações em outros domínios de segurança.

Se de um lado essa evolução tecnológica possibilita melhoria e agilidade nos processos da organização, de outro, essa evolução e dependência da tecnologia fazem surgir ameaças que até então não existiam e que, caso sejam concretizadas, podem causar danos irreparáveis ao negócio. Com isso, a preocupação dos gestores dos processos aumenta a cada dia no sentido de identificar possíveis impactos, sejam eles legais, de imagem, financeiros e operacionais, causados por ameaças que exploram as vulnerabilidades existentes nos ativos que suportam os processos de negócio.

No mundo dos negócios, a aplicação de Tecnologia da Informação (TI) é cada vez mais relacionada à competitividade das empresas. A globalização aumentou a competitividade e exigiu que as empresas modernizassem seus processos e a relação com os seus clientes.

Isso vem exigindo que a TI responda às demandas do negócio, legais e regulatórias em velocidade cada vez maior. A Tecnologia da Informação (TI) que suporta o ambiente de negócio está cada vez mais complexa e com diversas variáveis que promovem um ambiente com mais vulnerabilidade e exposição das informações corporativas.

Associada a esse cenário, a interatividade das soluções de TI, além de ser um requisito obrigatório, acarreta uma velocidade crescente das operações e transações no mundo dos negócios. A confidencialidade, integridade e disponibilidade da informação, o atendimento aos requisitos legais e regulatórias, além de serem exigências para as empresas, precisam ser evidenciados.

A Figura 3 apresenta o contexto geral em uma organização e Figura 4, o contexto global.

## 3. Compreendendo a abrangência do cenário da guerra cibernética

Incidentes de segurança ocorrem a todo instante e podem trazer impactos de toda a sorte (financeiros, operacionais, ambientais, legais, imagem, etc.), e, conforme o caso, os danos podem ser irreparáveis. Uma organização pode estar sofrendo nas mãos dos atacantes cibernéticos neste momento. A cifra que envolve essa batalha pode superar a casa de dezenas de trilhões de dólares nos próximos anos. O mundo dos negócios nunca experimentou uma guerra como essa, diferente de tudo o que já vivemos.

É uma batalha desigual - o atacante tem clara e nítida vantagem. Os defensores têm de proteger um perímetro abrangente e complexo (ver Figura 4), enquanto o atacante só precisa encontrar uma brecha na proteção cibernética implantada e infligir danos reais. Essa guerra cibernética desigual pode ser verificada quando olhamos para a estrutura de custos que coloca a vantagem também para o atacante. Ou seja, os esforços financeiros e de tempo do atacante são relativamente pequenos para desenvolver um novo ataque, enquanto os defensores têm que investir milhões para implementar uma possível proteção contra esse novo ataque.

O crime cibernético e seus atores são organizados e colaboram um com o outro, o que torna essa situação ainda mais complexa para os defensores. Os atacantes são, na sua grande maioria, talentosos engenheiros com uma compreensão profunda do meio ambiente que estão atacando. Muitas vezes, o entendimento dos atacantes excede o dos indivíduos que estão operando as estruturas tecnológicas que suportam o alvo. O crime cibernético e seus atores operam globalmente em um

**Figura 3 - Adaptada a partir da relação entre a Segurança Cibernética e outros domínios de segurança descrita na norma ISO/IEC 27032:2015 - Tecnologia da Informação - Técnicas de Segurança - Diretrizes para Segurança Cibernética**

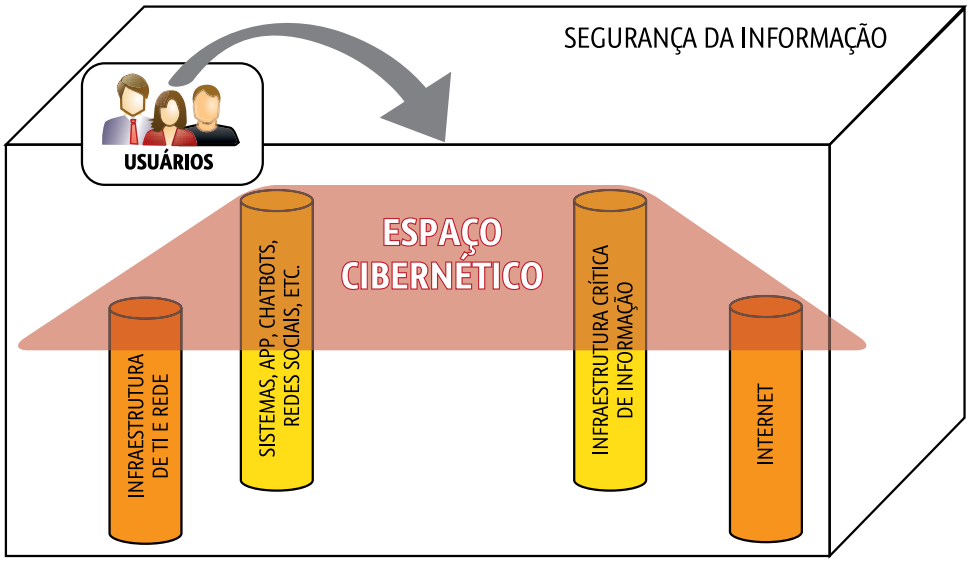
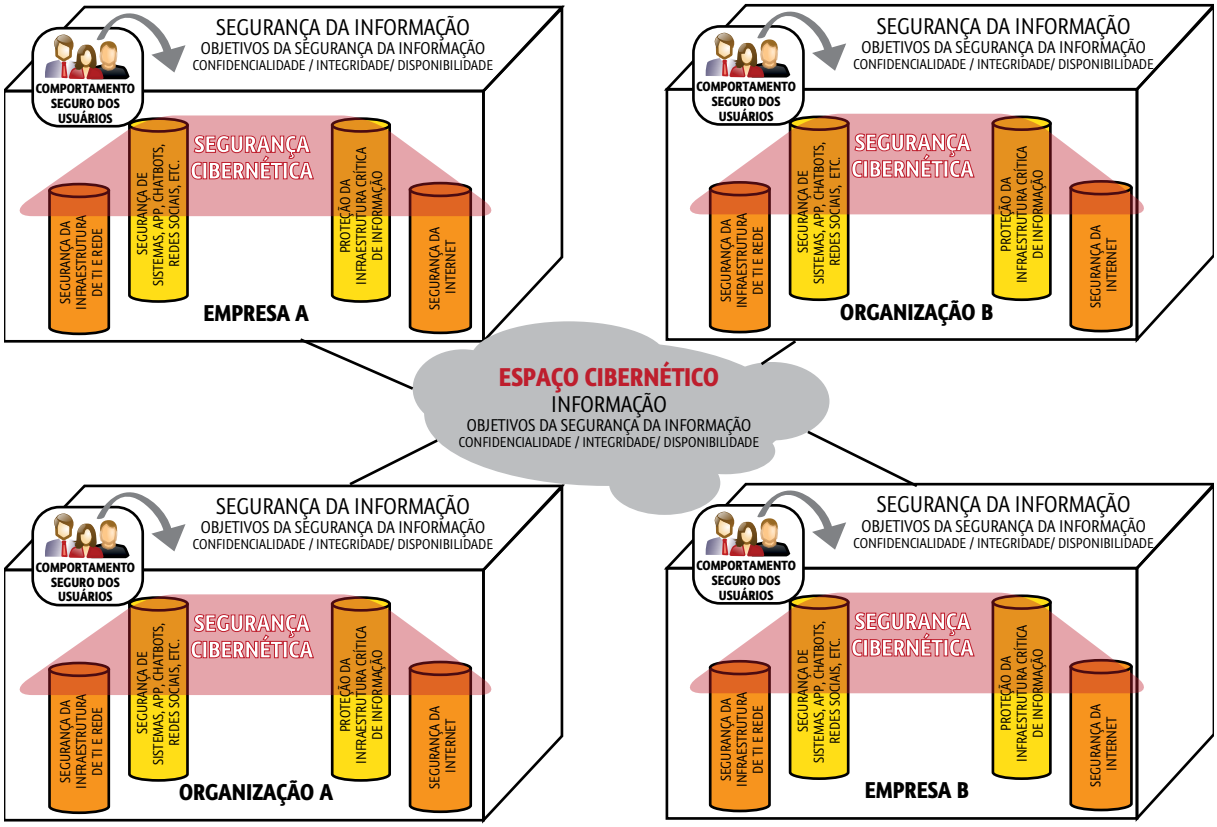


**Figura 4 - Exemplo do contexto global da segurança cibernética**




ambiente de baixo risco e com pouca chance de serem descobertos e pegos. Quando isso ocorre, a punição é leve. É necessária uma coordenação internacional, o que raramente ocorre, para obter uma pequena vantagem na luta contra esse sombrio inimigo mal definido e não identificado.

A amplitude e diversidade dos cenários da guerra cibernética vêm aumentando em decorrência de adoção de novas tecnologias e como essas são utilizadas nos negócios. Estas novas tecnologias acarretam outras vulnerabilidades e potencializam novos alvos. Os dispositivos como internet das coisas (Internet of Things – IoT), telefones inteligentes e tablets, utilizando tecnologia de acesso sem fio que acessam aplicativos baseados em nuvem, oferecem inúmeras oportunidades para os atacantes. A conectividade da internet penetrante amplia ainda mais o alcance do atacante. O vandalismo cibernético, que começou há pouco mais de três décadas, cresceu de forma severa para incluir atos de espionagem, extorsão e outras formas de crime organizado.

Pretendemos, neste artigo, explorar o campo de batalha da segurança. Dedicamos muito dos nossos dias trabalhando com as empresas para ajudá-las a melhorar a governança e a postura de segurança com a finalidade de proteger os valiosos ativos, segundo a visão do negócio, não interferindo na velocidade com que as atividades empresarias ocorrem. Diante da crescente incerteza nos negócios e do cenário da guerra cibernética, é possível afirmar que, se continuarmos nessa trajetória e com as abordagens atuais, vamos continuar perdendo as batalhas e provavelmente a guerra.

## 4. Devemos mudar a abordagem?

Nas últimas duas décadas e particularmente na última, de forma geral e com raríssimas exceções, as organizações de segurança e as ações/projetos de segurança, nos governos e nas empresas públicas e privadas, focaram na tecnologia de maneira excessiva, e, conforme o caso, exclusivamente em tecnologia. Endereçaram investimentos e esforços na construção de camadas (mais fortes, mais altas e mais largas) de proteção tecnológica cada vez maiores, considerando, de forma equivocada, que a as camadas de fortificações adicionais seriam suficientes para alterar a situação da guerra cibernética nos dias de hoje.

Em outras palavras, o movimento para promover a segurança está centrado na tecnologia. É claro que tudo isso é necessário. Para usar armas mais potentes, é preciso a implantação correta no campo de batalha para que elas possam ser efetivas. Observando as grandes brechas organizacionais, nos últimos cinco anos, podemos perceber que a maioria delas poderiam ser evitadas com a tecnologia de segurança existente e em uso no mercado há pelo menos seis anos.

A percepção é que as organizações realizam altos investimentos em ações e projetos de segurança todos os anos e parece que a proteção não está sendo efetiva, pois os incidentes, de menor ou maior impacto, continuam a acontecer em cenários de segurança em que, em teoria, não deveriam acontecer. Nós conhecemos organizações com excelentes profissionais que diariamente são desafiados com a tarefa de proteção e buscamos compreender por que eles estão perdendo essa luta. Isso vem consumindo grande parte do nosso tempo, avaliando, estudando e debatendo se essa guerra não é invencível e que o melhor cenário esperado é aquele com redução de incidentes na linha do tempo, ou se existe um caminho melhor para enfrentar esse desafio da proteção.

O nosso foco tem sido nas questões que ajudam e/ou contribuem para criar um clima de esperança para equilibrar essa guerra:

- Por que as organizações reconhecidas pelas suas competências e capacidades de desenvolver e realizar uma gestão bem-sucedida de riscos, em ambientes altamente adversos, com base em estratégias efetivas de mitigação desses riscos, não conseguem desenvolver um melhor trabalho para garantir uma proteção adequada dos recursos e ativos de informação?

- Por que as organizações que conseguem mudar o curso da história e que têm competência e capacidade não conseguem ser efetivas na construção de defesas bem-sucedidas?

As grandes lideranças dessas empresas, responsáveis pelo desenvolvimento de estratégicas fundamentais para o "core" do negócio, e com conhecimento profundo sobre o negócio deveriam incluir no seu trabalho também o foco na área de segurança, adotando uma nova abordagem para segurança da informação nas organizações, como, por exemplo:

- Trabalhar diretamente com executivos, donos de missão / negócios e gerentes de programas;

- Trazer todas as partes interessadas à mesa com interesse no sucesso ou no resultado da missão ou da função comercial;

- Considerar os requisitos de segurança da informação como requisitos funcionais comuns;

- Realizar análises de trade-of de segurança no que se refere aos custos, cronograma e requisitos de desempenho;

- Implementar métricas para executivos-chave.

## 5. Desafios para a segurança cibernética[5]

A evolução nos métodos de comunicação nos últimos anos trouxe inúmeros benefícios. Cada vez mais organizações, negócios e cidadãos estão conectados através de novos canais e aplicações do que jamais seriam imaginados poucos anos atrás. Os negócios se tornaram extremamente dependentes da rápida troca de informação, que, em grande parte, ocorre por meio da internet em função da grande conveniência dessa abordagem. Entretanto, não há apenas benefícios nessa globalização e interconexão dos negócios - novas ameaças e vulnerabilidades também emergem como parte desse processo.

Os ataques cibernéticos mais modernos podem comprometer informações sensíveis, causando prejuízos financeiros e de imagem. Vale lembrar que a infecção do ransomware WannaCry se iniciou em 12 de maio de 2017 e muito rapidamente já havia se espalhado por mais de 200 países, com mais de 200.000 casos registrados. Em 27 de junho, ocorreu a infestação do Petya, outro ransomware. Corporações de todo o mundo (inclusive no Brasil) foram afetadas por esses códigos maliciosos, que criptografam dados de sistemas corporativos, tornando-os indisponíveis para seus próprios donos até que um "resgate" seja pago aos atacantes em forma de moedas virtuais (bitcoins), sendo que, mesmo quando o resgate é pago, não há garantia de recuperação.

Muitos ataques podem ser executados remotamente e de modo silencioso, tanto por pessoas localizadas na própria organização quanto por atacantes completamente anônimos. As fontes de ameaças em potencial e as motivações para tais atos são muitas, e o rastreamento preciso dos autores de ataques cibernéticos normalmente não é uma tarefa simples. Em cenários mais críticos, os ataques podem até mesmo colocar vidas humanas em risco (desativação de plantas de energia e ataques em outras infraestruturas críticas). De fato, existe uma preocupação cada vez maior com o uso do espaço cibernético para ações terroristas. Tanto redes governamentais quanto de empresas privadas estão em risco, e o nível regulatório (leis) e acordos internacionais em termos de cibersegurança ainda são insuficientes.

O espaço cibernético oferece oportunidades para terroristas executarem atos disruptivos e de elevado impacto financeiro. Diferentemente de explodir um avião ou matar reféns, interromper o fluxo de informações pode infligir dor suficiente para passar a mensagem simbólica central do terrorismo, sem necessidade de recorrer aos aspectos tradicionais do terrorismo destrutivo.

Também é importante ressaltar que a necessidade de segurança vai além dos problemas puramente tecnoló-

5 Reproduzido do White Paper "Defesa cibernética com os controles críticos de segurança do CISTM (Center for Internet Security)", item 2, Módulo Security Solutions, junho de 2017, versão 1.2

gicos que envolvem hardware, software e ataques que exploram vulnerabilidades inerentes ao TCP/IP. Parte do problema, em muitas organizações públicas e privadas, se deve à falta de políticas e regulamentos adequados, ou de aderência (conformidade) a essas políticas, quando existem. Acima de tudo, há o problema comportamental: as pessoas são o link mais frágil da cadeia de segurança da informação. Firewalls, scanners de vulnerabilidades, sistemas de detecção de ataques, SIEMs não oferecem proteção contra ataques de engenharia social. O já mencionado ataque do ransomware WannaCry e outros tipos de malware podem utilizar a engenharia social como um vetor, através do envio de anexos ou links maliciosos em e-mail, mesmo em empresas que possuem softwares antiphishing instalados. Tradicionalmente, a defesa cibernética não aborda esses aspectos que têm caráter puramente tecnológico, que envolvem políticas, compliance, educação e conscientização de usuários, que fazem parte do escopo mais amplo da Segurança da Informação, mas, na prática, essas questões precisam ser endereçadas através de controles complementares.

Resumindo, o risco é real e as repercussões são graves. Diante desse cenário, implementar um programa efetivo de segurança cibernética é um dos principais desafios que organizações públicas e privadas enfrentam na atualidade. Muitas dessas organizações não têm sequer conhecimento dos riscos a que estão sujeitas por não estarem implementando defesas adequadas, contra-ataques cibernéticos que podem afetar a confiabilidade, integridade e/ou continuidade de serviços críticos e outros problemas, como danos à reputação e roubo de propriedade intelectual. É nesse contexto que se compreende a extrema relevância dos TOP 20 Critical Security Controls propostos pelo CIS[6].

## 6. Modelo de governança corporativa de segurança organizacional

> "The art of war teaches us to rely not on the likelihood of the enemy's not coming, but on our own readiness to receive him." (Sun Tzu)

A capacidade efetiva de governar a segurança em uma organização, avaliando os seus riscos e implementando as medidas de segurança que a protejam contra a exploração é o que chamamos de comportamento (postura) de segurança organizacional. A governança, gestão e operação corporativa de segurança são suportadas por elementos estruturais de segurança chaves. As ferramentas e processos de segurança são elementos estruturais fundamentais e são referenciados como controles pela indústria de segurança. Um controle pode ser um dispositivo de prevenção de intrusão de rede, que garante mais robustez às redes, filtrando as transmissões das comunicações suspeitas e/ou as perigosas já conhecidas, nesse caso, esse dispositivo é um controle técnico, ou seja, centrado na tecnologia. Um outro controle poderia ter mais foco no processo, como, por exemplo, o processo de gerenciamento de mudanças, usado para gerenciar as mudanças, de qualquer natureza, em um processo do negócio, nas atividades, nas aplicações, nos ativos de informação e até mesmo no ambiente organizacional, evitando os riscos à quebra de segurança decorrentes de alterações que ocorrem no dia a dia em atendimento à dinâmica da TI e dos Negócios. A implementação e implantação desses controles devem considerar os requerimentos e as necessidades da organização em termos de custo, impacto no negócio e efetividade final do controle.

Observando os padrões existentes, percebemos que a maioria faz um excelente trabalho em relação à avaliação de controles e metodologia. Entretanto, não apresenta considerações em relação a itens críticos e relevantes como custos de implementação, manutenção e evolução, além de não incluir a capacidade geral de gerenciamento e retorno para a organização.

É fundamental determinar se o comportamento organizacional de segurança é efetivo. Portanto, é necessário utilizar algum método para que a organização possa determinar se a sua postura de segurança organizacional é efetiva, com o uso de um modelo de maturidade que forneça um método que, aplicado às disciplinas específicas de segurança, possibilite a medição de sua maturidade. Ao medirmos a maturidade das disciplinas de segurança, podemos determinar se elas implementam um comportamento de segurança organizacional efetivo e, com isso, medir a maturidade da governança corporativa da segurança da informação. Não importa qual é o framework que suporta o modelo de governança de segurança adotado, o que importa é se esse framework disponibiliza um método para obter a maturidade das disciplinas de segurança da informação. Ao avaliar a maturidade dessas disciplinas, podemos determinar seus níveis de maturidade.

Os níveis de maturidade, do menor para o maior, poderiam ser: Inexistente, Inicial, Repetitivo, Definido, Gerenciado-Proativo e Otimizado, com os seguintes significados:

- **Inexistente** - Não existem controles formais e as respostas a ocorrências de segurança da informação são reativas, tempestivas e não um processo formal de detecção e resposta a incidente. Não há percepção da efetividade da proteção implantada.

- **Inicial** - Os processos são informais e não há padrões. Os problemas são conhecidos pela área de segurança e o gerenciamento da segurança é desorganizado e focado apenas na TI, sem alinhamento com

6 The CIS Critical Security Controls for Effective Cyber Defense - https://www.sans.org/critical-security-controls. Acessado em: out. 2017.

os riscos do negócio. Os controles não são confiáveis ou não representam a efetividade da proteção.

- **Repetível -** Controles e processos padronizados não formalizados. Falta comunicação formal. Os controles são obtidos de forma isolada e não refletem as mudanças da tecnologia.

- **Definido -** Os processos e controles implantados e formalizados e a comunicação já estão definidos. A capacidade de segurança amadurece em função da repetição e dos processos padronizados. Esses processos podem ser orientados no atendimento de requisitos de conformidade legal ou padrões normativos externos ou pela padronização a partir de políticas e normas internas. Não há uma governança de segurança centralizada. O alinhamento dos processos com os requisitos de segurança irá depender dos indivíduos da equipe de segurança. Adota-se como regra o uso aceitável de um padrão de procedimentos operacionais e um padrão de ambientes operacionais. Não há ferramentas de gestão e integração da situação da segurança da informação com o negócio.

- **Gerenciado-proativo -** Processos em aperfeiçoamento já fornecem as boas práticas. Há capacidade para orientar a segurança para o futuro, o nível de maturidade aumenta em função da capacidade reativa baseada em regras. A governança centralizada fortalece-se e as táticas de curto prazo são substituídas por estratégias de longo prazo. O atendimento à regulação normativa é melhor compreendido e provisionado de forma mais eficaz. O ganho de eficiência organizacional e a redução do tempo de resposta ocorrem devido à gestão situacional da segurança integrada. Os controles são alinhados a partir dos riscos do negócio.

- **Otimizado -** Os processos, padrões e controles de segurança da informação estão integrados e há capacidade de governança e gestão organizacional da segurança. A eficiência é percebida quando os componentes tecnológicos e de processos são automatizados e integrados, aumentando a precisão e diminuindo o custo de gerenciamento do ambiente de segurança. A integração da consciência situacional da organização com o ambiente de segurança permite que a organização compreenda a situação rapidamente e possa adaptar-se instantaneamente ao enfretamento das ameaças. Os riscos do negócio são os principais fatores para o alinhamento com as iniciativas de segurança. A melhoria contínua da qualidade é primordial, e os processos existem para garantir que a informação do evento de violação seja distribuída formalmente. A organização dispõe de um processo contínuo para revisão de sua estratégia de segurança e os níveis funcionais participam e avaliam a situação de segurança da informação alinhada aos processos do negócio.

É importante compreender que o processo de maturidade é evolutivo. Nós não acreditamos que o pular etapas do modelo de maturidade irá proporcionar a evolução esperada.

## 7. Desenvolvendo a estratégia

Não é raro uma sessão de planejamento ser mais focada na análise de gaps do que no desenvolvimento de um verdadeiro plano estratégico. De forma geral, a equipe de segurança, por diversas razões válidas, desenvolve seus planos de ação baseados na sua capacidade de se defender contra as ameaças ou ataques genéricos e relacionados com a brechas conhecidas de seus controles.

O plano de ação resultante certamente não é um plano estratégico, pois falta um elemento fundamental: a compreensão explícita dos ativos de informação da empresa que precisam ser protegidos. Sem esse elemento, a segurança não consegue avaliar se os controles são adequados, inadequados ou sofisticados, e a consequência da ausência do alinhamento entre os riscos empresariais específicos e os controles de segurança é que o plano de ação não poderá ser otimizado.

A essência do planejamento estratégico é bastante simples: descubra onde você está e onde você quer estar, e descubra quando e como chegar lá. Mas, embora a essência seja simples, a construção de um plano estratégico para a segurança requer um grande esforço. Os planos definem o que será feito sem indicar como isso será feito. Os planos estratégicos também identificam indicadores-chave para que eles possam ser medidos, gerenciados e contribuir para a garantia de que estão na direção certa. Em nossa experiência, as organizações de segurança raramente possuem planos estratégicos de segurança completos e atualizados. Para algumas organizações, as reações táticas aos incidentes é o padrão. O chamado plano é o reagir após uma quebra de segurança, o que significa: nenhum plano. Há casos de uso de incidentes de segurança para obtenção de recursos financeiros e garantir o apoio de executivos para realizar as mudanças na organização.

## 8. Para refletir

- Gap Analysis de segurança focado na tecnologia não deve ser o único elemento a direcionar o plano estratégico de segurança.

- Implementar a governança, gestão e operação da segurança alinhada, desde o início, com os riscos do negócio conseguirá o suporte global da organização, terá a abrangência e capacidade necessárias para o sucesso.

- As entregas e o processo de planejamento da segurança devem garantir a proteção requerida pelo negócio.

- O plano estratégico de segurança deve explicitar se o nível de proteção é proporcional aos impactos decorrentes de uma quebra de segurança.

**Referências**


ABNT NBR ISO/IEC 27032:2015 - **Tecnologia da Informação - Técnicas de segurança - Diretrizes para segurança cibernética**

**The Center for Internet Security Critical Security Controls**. Disponível em: http://www.cisecurity.org/critical-controls.cfm. Acessado em: out. 2017.

CLARKE, R. and KNAKE, R. **Cyber War**. Ecco, 2010.

ARQUILLA, J. and RONFELDT, D. **The Advent of Netwar.** RAND (National Defense Research Institute), 1996.

**The CIS Critical Security Controls for Efective Cyber Defense Version 6.1** - Center for Internet Security. August 31, 2016.

**CIS Controls - Follow our prioritized set of actions to protect your organization and data from known cyber attack vectors**. Disponível em: https://www.cisecurity.org/controls/. Acessado em: out. 2017.

**CIS Controls - Mapping and Compliance**. Disponível em: https://www.cisecurity.org/cybersecurity-tools/mapping-compliance/. Acessado em: out. 2017.

ISO / IEC 27000:2014 - **Information security management systems** – Overview and vocabulary.

NBR ISO / IEC 27001:2013 – **Sistemas de gestão de segurança da informação** - **Requisitos.**

NBR ISO / IEC 27002:2013 – **Código de prática para a gestão da segurança da informação.**

Norma ISO 27005:2008 - **Técnicas de Segurança – Gestão de riscos de segurança da informação;**

ABNT ISO/IEC 27014:2013 **Tecnologia da Informação Técnicas de Segurança Governança de segurança da informação**

Norma ISO 27031:2015 – **Tecnologia da Informação – Técnicas de segurança – Diretrizes para a prontidão para a continuidade dos negócios da tecnologia da informação e comunicação.**

Norma ISO 31.000:2009 - **Gestão de Riscos – princípios e diretrizes**

ABNT ISO/TR 31004:2015 **Gestão de riscos Guia para implementação da ABNT NBR ISO 31000**

ABNT NBR ISO/IEC 31010:2012 **Gestão de riscos Técnicas para o processo de avaliação de riscos**

Norma ISO/IEC 22301 – **Código de Prática para a Gestão de Continuidade de Negócios;**

Norma ISO/IEC 20000 - **Sistema de Gerenciamento de Serviços de TI;**

Norma ISO/IEC 38500:2009 – **Governança Corporativa de Tecnologia da Informação;**

COBIT 5- **Control Objectives for Information and related Technology;**

ITIL v3 – **Information Technology Infrastructure Library;**

VAL IT – **Enterprise Value: Governance of IT Investments;**

**Código de melhores práticas de governança corporativa – IBGC**;

BEERNSTEIN, Peter L. **Desafio aos deuses, a fascinante história do risco**. Campus, 1996.

**White Paper "Defesa Cibernética com os Controles Críticos de Segurança do CISTM (Center for Internet Security)"**, item 2, Modulo Security Solutions, Junho de 2017, Versão 1.2

CHARAN, Ram. **Ataque! Transforme incertezas em oportunidades**. HSM, 2016.

WESTMAN, George; HUNTER, Richard. **IT Risk, Turning business threats into competitive advantage**. Harvard Business School Press, 2007.

# Segurança em votações eletrônicas utilizando protocolos blockchain

Arquivo pessoal


## *Rafael de Freitas Setragni*

*Bacharel em Sistemas de Informação pela Pontifícia Universidade Católica de Minas Gerais (PUC-MG) e técnico em Eletrônica pelo Centro Federal de Educação Tecnológica de Minas Gerais (Cefet-MG). Atualmente trabalha com desenvolvimento de sistemas e soluções em segurança da informação da Prodemge.*



### *Resumo*

*Este artigo tem como objetivo solucionar os problemas da votação por meios eletrônicos, utilizando a tecnologia de protocolos das blockchains, um conjunto de algoritmos extremamente confiável utilizado no coração de todas as transações eletrônicas envolvendo moedas digitais. Após determinar os pré-requisitos de confiabilidade, integralidade e confidencialidade necessários para um processo eleitoral, serão analisadas as ameaças e possíveis fraudes do sistema atual e como um sistema de eleição por blockchain pode eliminar esses problemas, de forma transparente e auditável por qualquer cidadão.*



***Palavras-chave:***

*e-voting blockchain, merkle tree, proof of work, proof of stake, 51% attack, P2P, voto impresso, chaves públicas e privadas, criptografia hash, BIP38, QR Code, segurança da informação no sistema eleitoral.*


## 1. Usar ou não o voto impresso

Conforme a lei 13.165/2015, originada do PLC 75/2015, durante as eleições, a partir de 2018, juntamente com a votação na urna eletrônica, será impressa uma via em papel, na qual o eleitor poderá conferi-la através de um visor. Todo procedimento será realizado sem intervenção de terceiros, ou seja, o eleitor não levará para casa nenhuma cópia desse comprovante, garantindo o sigilo do voto. Entretanto, essa medida está sofrendo duras críticas e não encontra consenso entre os próprios senadores, mesmo depois de se tornar lei.

Analisando os argumentos, é possível encontrar razão para os dois lados. A eliminação do uso do papel segue uma tendência de evolução do sistema eleitoral. A facilidade e a velocidade da contagem e recontagem dos votos, especialmente em um país de dimensões continentais, são incomparáveis ao antigo sistema tradicional de votos em papel. Além disso, o voto digital não sofre tanto com problemas clássicos de transporte, panes elétricas, conservação e falhas humanas e mecânicas na contagem, como ocorre no meio físico.

Mas é inegável que a população demanda por mais confiabilidade no sistema eleitoral, especialmente após os diversos escândalos e denúncias recentes do sistema político. Até mesmo o meio digital está com a própria confiabilidade em xeque. De acordo com a Kaspersky, é estimado que cerca de 30% dos internautas brasileiros são afetados por malwares, botnets e softwares maliciosos. Além disso, ataques e vazamentos de informações digitais em grandes empresas de renome são recorrentes e conhecidos pelo público.

Nesse cenário, apenas a palavra do Tribunal Superior Eleitoral (TSE), órgão responsável pelo processo elei-

*Urna eletrônica com impressão de comprovante, conforme a lei 13.165/2015*

*Imagem retirada do site: https://www12.senado.leg.br/noticias/materias/2016/02/23/voto-impresso-comeca-a-valer-em-2018-mas-ja-e-alvo-de-criticas*

toral, não é mais o bastante para trazer tranquilidade ao cidadão. Afinal, o poder de quem vota é anulado se quem conta os votos está corrompido. É preciso criar mais meios de assegurar e auditar o sistema eleitoral, não só para fazer o sistema em si ser mais justo, quanto para contribuir com a recuperação da confiança da população no meio político.

O discurso dos que defendem o uso do comprovante em papel aponta que a impressão do voto em meio físico cria redundância no registro dos votos, podendo ser utilizada para recontagem em casos de suspeitas e, assim, prevenir possíveis fraudes no meio eletrônico. Portanto, quem tiver a intenção de manipular os resultados do sistema eleitoral terá que fazer isso tanto no meio físico quanto no meio digital, o que dificultaria a fraude.

Porém, usar o comprovante em papel praticamente elimina todos os benefícios do voto eletrônico. O registro no meio físico pode sofrer danos não intencionais por conservação e transporte. O sistema de impressão pode sofrer falhas mecânicas e demandar manutenção, atrasando o processo eleitoral. Fraudes ainda podem ocorrer. O comprovante físico pode ser alterado, substituído, desviado, destruído, e a segurança da redundância daquele voto, que é visto pelo eleitor apenas uma única vez na vida, depende da confiança do mesmo grupo de pessoas que está encarregado da segurança do meio digital do qual é questionado.

Não só isso, mas o processo de recontagem do meio físico também pode ser corrompido e sofrer falhas intencionais e não intencionais. Mesmo se tratando de um processo mais custoso pela redundância do voto impresso, o sistema eleitoral proposto ainda é corruptível e, envolvendo tantos interesses e cifras na casa dos milhões e bilhões, incentivos e recursos para a fraude ainda são presentes e alcançáveis por parte dos interessados.

Assim, mesmo sendo claramente necessário o comprovante em papel, como proposto, a medida ainda não é o bastante para trazer segurança para o sistema eleitoral que a população demanda. O fato de o registro do voto também ser em meio físico não é, por si só, garantia de fraude. Para esse objetivo ser atingido, de forma definitiva, o processo eleitoral deve transcender os indivíduos e organizações e ser transparente e auditável por qualquer um, inclusive pelo próprio eleitor, a qualquer momento e quantas vezes forem necessárias.

## 2. Entendendo o problema

Antes de propor e analisar uma possível solução, é preciso ter em mente quais são as regras que compõem uma eleição e quais são os problemas a serem sanados. É claro que não existe um sistema 100% seguro ou mesmo que tenha todas as suas falhas conhecidas. Portanto, este artigo buscará levantar um número considerável de falhas para então propor um modelo melhor e aceitável.

- O processo eleitoral deve oferecer redundância dos votos, em diversos meios, tanto físicos quanto digitais, visando encarecer e dificultar as fraudes.
- Cada eleitor deve votar somente uma vez.
- O voto deve ser sigiloso, não sendo possível para um terceiro correlacionar o voto com quem votou.
- O voto deve ser auditável, ainda assim impedindo que um terceiro utilize esse mesmo processo de auditoria para quebrar o sigilo dos votos individuais.
- O voto deve ser escasso. Portanto, não deve ser possível criar eleitores fantasmas, tendo em mente que são necessários apenas dois eleitores fantasmas para invalidar um real e apenas a quantidade mínima para eleger o candidato alvo e mudar os resultados da eleição.
- O voto não pode ser alterável, em nenhum momento, e não pode ser realizado por alguém diferente do eleitor.
- O próprio sistema de votação deve ser auditável por qualquer um.
- O processo de contagem dos votos deve ser feito de forma segura, com o mínimo de erros de contagem e permitindo recontagem.

É importante ressaltar que o processo eleitoral, por fazer uso do meio físico e digital, reúne os atributos que permitem todos os ataques clássicos tratados na ciência de segurança da informação. Portanto, o processo eleitoral pode:

- Sofrer ataques silenciosos, buscando fraudar o sistema e modificar o resultado sem que seja detectado.
- Sofrer ataques aberrantes, buscando destruir a credibilidade do processo, forçando o sistema antigo e já conhecido pelo atacante a permanecer em vigor.
- Sofrer ataques de negação de serviço, sobrecarregando o sistema e inviabilizando o próprio uso.

Um processo eleitoral é composto por três pontos de falha críticos: o registro do voto, o transporte dos votos e o processo de contagem dos votos. Basta que apenas um desses três pontos de falha seja manipulado para que todo o processo seja comprometido.

Ao alterar o próprio registro dos votos, mesmo com o transporte e a contagem adequados, o resultado é

comprometido. Ao comprometer o transporte, os votos podem ser trocados e, mesmo com o registro dos votos corretos e a contagem, o resultado é comprometido. E, ao fraudar a contagem, mesmo com o registro e transporte dos votos garantidos, o resultado final é comprometido.

Em um mundo ideal, todo o processo eleitoral e os elementos que o constituem devem ser auditados por qualquer cidadão, a qualquer momento. E esse estado ideal é totalmente coberto pela tecnologia de blockchain.

## 3. Os benefícios do uso de blockchains no registro do voto

O sistema eleitoral proposto ocorre, quase que em sua totalidade, no meio digital, possuindo redundância tanto física quanto digital por posse do eleitor e por diversos nodos espalhados pela rede de computadores, de forma transparente, computacionalmente segura e auditável por qualquer um.

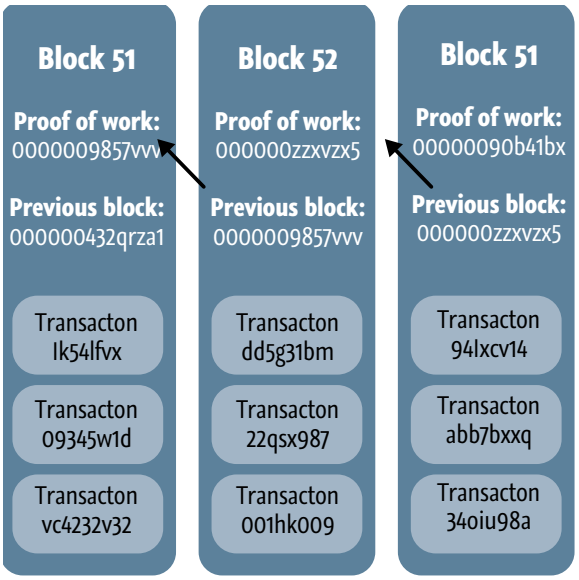
Esse sistema é possível graças ao uso do protocolo chamado blockchain. Uma blockchain é um conjunto de várias tecnologias, sendo, de forma simples e generalizada, um banco de dados de domínio e acesso público, contendo todas as transações realizadas desde o seu princípio salvas em blocos, replicados entre diversos computadores diferentes que se comunicam, por meio da tecnologia P2P (Peer-To-Peer). Dessa forma, na blockchain não existe um único servidor, pois todos os computadores são considerados como servidores e podem sair e entrar sem prejudicar os demais.

Nessa rede, como cada computador pode pertencer a qualquer um e não existe nenhuma inspeção ou pré-requisito para funcionar, é assumido por princípio que cada computador não é considerado como confiável, mas devido às regras de relacionamento entre eles e o nível de dificuldade de alterações fraudulentas, que as informações armazenadas na blockchain são muito seguras.

O termo blockchain vem do conceito de que cada computador da rede P2P, chamado de nodo, captura e armazena todas as transações realizadas na rede em blocos limitados a 1 Mb de espaço (no caso da bitcoin, sendo cerca de 1.800 até 2.500 transações). Esses blocos são ligados entre si, do mais antigo para o mais atual, em pilhas formando uma corrente.

É importante ter em mente que cada nodo da rede irá capturar as transações em uma ordem diferente umas das outras, dependendo da sua posição. Após encerrar a captura das transações o bastante para ocupar quase todo o espaço do bloco, o nodo encerra o bloco que construiu escrevendo uma hash criptográfica para ser a sua assinatura digital.

**Figura 1 - Exemplo de ligação dos blocos de dados de uma blockchain**




*http://dataconomy.com/2015/10/wtf-is-the-blockchain-a-guide-for-total-beginners/*

Uma hash criptográfica é um conjunto de letras, números e símbolos, gerado a partir de uma função matemática complexa. Essa função matemática tem como objetivo garantir três propriedades:

1. O texto resultado terá sempre um tamanho fixo, independentemente do tamanho da informação utilizada como base.

2. Caso a informação de base sofra uma modificação, mesmo que mínima, o texto resultante será completamente diferente.

3. Não é possível chegar ao texto original a partir do texto resultante da função hash.

No caso da blockchain, o texto de referência é composto por todas as transações do bloco (incluindo a transação de recompensa, que será explicada mais adiante), uma palavra base qualquer, uma cópia da assinatura digital do bloco passado e a sua própria assinatura digital, gerada a partir de todas as informações do bloco. Isso não só garante que o conteúdo do bloco não será alterado, quanto também o do bloco anterior, e assim por diante.

## 4. Proof of work vs. proof of stake

Para prevenir que muitos blocos concorrentes sejam gerados ao mesmo tempo ou mesmo que um atacante tenha facilidade em tentar fraudar a rede, um bloco só pode ser considerado como válido caso a hash da assinatura digital siga um critério preestabelecido, que demande uma certa dificuldade matematicamente es-

perada, para ser encontrada. Essa é considerada como a prova de trabalho (ou proof of work, do inglês) que cada bloco deve ter para provar o seu valor e sequer ser considerado pelos outros nodos da rede.

No bitcoin, como exemplo, a hash de prova de trabalho gerada deve conter um número de zeros iniciais para ser considerada como válida. Devido a três propriedades garantidas por uma função hash criptográfica, o bloco só poderá ser fechado modificando a palavra base para que o resultado da função hash tenha o número de zeros solicitado.

Então, todos os nodos da rede, cada um com posse do seu bloco contendo a ordem que receberam as transações mais a sua palavra base de escolha, começam a variar essa palavra a fim de encontrar a sua própria hash válida. Quando um bloco válido é encontrado, o nodo vencedor divulga o seu bloco e então este é adicionado à blockchain de todos os demais.

Como recompensa pelo feito, o bloco vencedor contém uma transação adicional, da qual adiciona novos bitcoins a uma conta escolhida. Esses bitcoins são, em parte, uma pequena percentagem de todas as transações do bloco, mas também de bitcoins "brindes", vindos de nenhuma outra conta. Pelo fato de os nodos conseguirem encontrar bitcoins novos através do seu trabalho, esses são apelidados de mineradores.

No protocolo da blockchain, é definido que a quantidade de novas moedas cedidas pela premiação diminui com o passar do tempo. Isso garante que a quantidade de bitcoin circulando pela rede é finita. Portanto, a moeda é garantida como escassa e não sofrerá tanta inflação pela criação de dinheiro adicional. Essa recompensa também não pode ser gasta antes de, pelo menos, 100 transações, para garantir que a nova moeda não perderá rastro, caso o bloco inicial seja destruído em uma falha.

Também a quantidade de zeros iniciais é aumentada com o passar do tempo, para assim garantir que o trabalho necessário para alguém encontrar a sua hash válida leve cerca de dez minutos, mesmo com a criação de computadores cada vez mais potentes ou especializados no cálculo da sua operação.

Sendo assim, considerando essas características, para alguém mal-intencionado alterar um dos registros de uma blockchain, será necessário recalcular todas as chaves de criptografia até o bloco inicial, chamado de gênesis. Caso contrário, toda blockchain se torna inválida e é automaticamente descartada pelos nodos da rede P2P.

Também é possível que o atacante substitua o bloco específico por outros dados, desde que o produto da função matemática hash utilizada na assinatura digital seja igual ao original e o gerado pelo próximo bloco. Isso é possível, pois as funções de hash criptográficas podem gerar o mesmo resultado para diferentes textos, ocorrendo colisões. Entretanto, a probabilidade de colisões utilizando funções hash fortes é vastamente remota.

Ainda que consiga, o atacante deverá ter o poder computacional de pelo menos 51% de todas as máquinas espalhadas pela rede P2P. Isso ocorre porque os nodos são programados para sempre manter a maior cópia de blockchain válida. Portanto, quando um fraudador cria um bloco válido novo, é extremamente provável que todos os outros computadores tenham conseguido ser mais rápidos e tenham criado uma blockchain válida maior.

Desse modo, considerando todas essas dificuldades, se torna caro demais para que um atacante obtenha êxito em alterar os dados de forma ilícita em uma blockchain. A matemática envolvida no fechamento dos elos da corrente garante que seja computacionalmente inviável fraudar o sistema, e o consenso de toda a rede é a garantia de segurança que as transações registradas precisam. Não é à toa que esse tenha sido o modelo adotado por todas as criptomoedas que atualmente circulam milhões e bilhões de dólares.

Entretanto, o uso de prova de trabalho tem os seus problemas. Analisando a rede da blockchain como um todo, o uso de prova de trabalho produz muito desperdício de energia elétrica no processamento das hashs e resfriamento das máquinas. Também, quanto mais profunda a transação ficar na blockchain, mais segura ela estará de ser descartada ou mesmo fraudada. O fato de cada bloco precisar de tanto tempo para ser gerado e adicionado na rede faz com que a demora para uma transação ser considerada como segura inviabilize o uso corriqueiro.

Também, a prova de trabalho apenas reduz a probabilidade de dois blocos válidos concorrentes serem gerados ao mesmo tempo, mas não elimina o problema. Quando isso acontece, ocorre uma falha conhecida como fork, que bifurca a rede bitcoin, fazendo com que transações válidas possam desaparecer. Mesmo com uma probabilidade insignificante, com infinitas e constantes tentativas, é esperado que um evento improvável ocorra, como é definido pela Lei de Murphy.

Visando solucionar essas dificuldades, a etherium, um dos modelos concorrentes de blockchain, propôs utilizar a prova de participação (ou proof of stake, do inglês) ao invés da prova de trabalho.

A prova de participação consiste que cada nodo da rede deve apostar créditos para participar da validação do bloco. Quanto maior a aposta e maior a posse de créditos de toda a rede, maior é a confiança que a rede tem

da sua participação e maior será a sua chance de vencer a corrida. Todavia, essa chance não é 100% garantida. Quando o bloco vencedor é gerado, os nodos checam a sua validade e, caso esteja tudo certo, o nodo vencedor leva todos os créditos apostados.

Isso torna a rede mais segura e veloz do que a rede defendida pela prova de trabalho. Os validadores que têm maior chance de vencer a corrida são os que não vão querer fraudar o próprio sistema, pois eles possuem muito dinheiro em jogo.

Como não é necessário gastar tanto tempo para processar o bloco de forma segura, mas, sim, créditos, o tempo de criação de cada bloco válido cai para frações de segundo, o que aumenta o throughput (vazão) da rede de forma considerável. No modelo de crédito atual, como as das companhias Mastercard e Visa, cerca de 2.000 transações podem ser realizadas a cada segundo em todo o mundo. Já na rede bitcoin, consegue-se processar cerca de 2.500 transações por segundo. Porém, graças ao uso da prova de participação, o número de transações por segundo da rede etherium passará para 1.000.000.

Considerando o ataque dos 51%, um dos ataques mais conhecidos e temidos das redes blockchains, no caso da prova de participação, o fraudador deverá possuir 51% de todos os créditos existentes para manipular os resultados. Esse montante torna improvável sequer a existência do atacante e, caso ele exista e erre o golpe, perderá não só tempo e processamento quanto uma boa porcentagem de todo o dinheiro investido.

Considerando todos esses fatores, o modelo de validação a ser adotado pelo sistema eleitoral deverá ser baseado, no mínimo, na prova de participação ao invés da prova de trabalho, pois aquela é mais segura, gasta menos recursos energéticos e é mais veloz em realizar o registro das transações. Também, o modelo de blockchain adotado deverá considerar que mesmo esse novo método de validação pode e deverá sofrer alterações com o tempo, ou mesmo ser completamente substituído por outro melhor.

Essas evoluções deverão ser consideradas e registradas já como parte do protocolo da rede a ser adotada. Caso contrário, o futuro da rede sempre será incerto e o consenso entre os mineradores pode não ser obtido, como ocorre com a blockchain do bitcoin ou litecoin, gerando novos forks e desvalorização da rede.

## 5. Contabilidade dos votos em tempo real, por qualquer um

Outro atributo importante das blockchains está no fato de que os seus dados são de domínio público, em que qualquer um em qualquer parte da rede pode replicar e auditar a integridade dos elos.

Em uma blockchain, não existe um único registro contendo o total que cada conta (ou endereço) possui. Esse valor é obtido contabilizando todas as transações anteriores direcionadas para aquele endereço desejado.

Dessa maneira, para determinar quanto cada carteira possui de forma eficiente, utiliza-se o conceito de armazenar em um local prioritário todas as transações que ainda não foram gastas.

Ao se realizar uma nova transação, a mesma é armazenada em dois locais: na blockchain geral e em uma área de acesso rápido. Quando existem transações futuras o bastante para totalizar o valor da transação de origem, esta passa a ser considerada como uma "transação gasta" e é removida da área de acesso rápido.

Essa área de acesso rápido geralmente ocupa 15% do total armazenado na blockchain e é formada por uma árvore binária, que usa como índice os endereços de destino. Dessa forma, é possível contar rapidamente o total que cada conta possui somando o valor das transações a partir do endereço desejado.

Isso possibilita que o resultado de uma eleição utilizando a tecnologia blockchain seja contabilizado e acompanhado pelos nodos da rede praticamente em tempo real. Basta atribuir a cada candidato um endereço virtual para o qual cada eleitor enviará o valor de sua carteira.

## 6. Auditoria dos votos computados pelo próprio eleitor

Em cada nova eleição utilizando-se a blockchain, será criada uma nova carteira digital para o eleitor, contendo o valor mínimo necessário para realizar uma única transferência.

Para garantir que apenas o eleitor possa realizar a transferência dessa carteira para os candidatos permitidos, e que seja feita apenas nos terminais autorizados, pode-se utilizar o conceito de chave privada e chave pública, em combinação com a criptografia BIP38 ou similar.

As chaves públicas e privadas são um par de hashes utilizadas no processo de assinatura digital. Combinando o dado desejado com os caracteres da chave privada, se produz uma assinatura digital de tamanho fixo que bate apenas com a chave pública. Com posse da chave privada, é possível descobrir a chave pública, mas não o inverso. A chave pública apenas permite checar a carteira digital e se alguma transação foi realizada.

Logo, basta gerar o conjunto de chaves públicas e privadas para cada nova carteira criada e passar a chave privada para o eleitor. Nesse caso, o TSE apenas manteria posse da chave pública.

Porém, com posse da chave privada, é possível transferir o valor da conta para qualquer outra conta que não seja dos candidatos.

Para garantir que isso não ocorra, a chave privada pode ser cedida pelo TSE por uma criptografia BIP38 que, por meio de uma palavra-chave, possibilita obter novamente o texto original.

No caso, o texto a ser protegido seria a chave de acesso privada da conta do eleitor e a palavra-chave do BIP38, formada por meio da combinação de uma senha do eleitor com outra senha aleatória, gerada no momento da criação da carteira digital, que ficará em posse do TSE. A palavra-chave do eleitor pode ser digitada ou mesmo preenchida automaticamente pela inserção de um terceiro dispositivo. Dessa maneira, somente o eleitor, com conhecimento da sua palavra-chave mais a palavra-chave do TSE, pode fazer a transferência do voto. Ou seja, a transação só ocorrerá com o consentimento dos dois.

Visando aumentar a redundância dos votos e dar a cópia do voto impresso que o eleitor tanto demanda, sem comprometer o sigilo do voto, pode-se utilizar o algoritmo de Árvore de Merkle.

Uma Árvore de Merkle é um algoritmo proposto por Ralph Merkle, em 1979, composto por uma arvore binária escrita das pontas até a raiz, em que cada nível é feito a partir da criptografia hash dos pares de filhos até o topo, chamado de valor raiz de Merkle. Sendo assim, segundo a terceira propriedade dos algoritmos de criptografia hash, qualquer modificação dos dados em qualquer um dos filhos da árvore altera completamente o valor raiz.

No caso de uma eleição, o eleitor recebe como comprovante do próprio voto uma cópia do valor raiz produzido pelo algoritmo de Merkle do seu bloco. Assim, é possível garantir que nenhum dado da transação foi alterado sem revelar a qual transação específica pertence o eleitor.

Para facilitar o uso do comprovante pelo eleitor, esse valor raiz da Árvore de Merkle pode ser fornecido por meio de um QR Code no comprovante.

O QR Code é uma evolução do código de barras tradicional, permitindo o armazenamento de longos textos com rápida leitura por qualquer dispositivo com câmera, como os smartphones modernos.

**Figura 2 - Exemplo de QR Code, que pode ser utilizado nos comprovantes eleitorais, digitais ou impressos.**

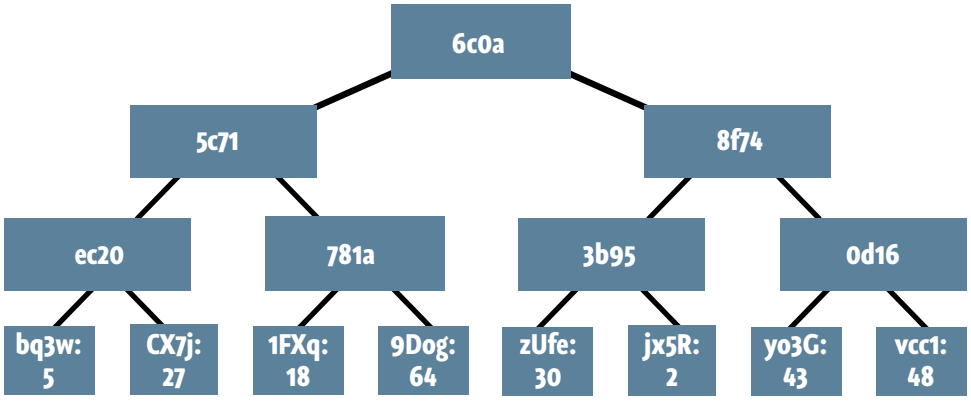
*Criada a partir do site http://br.qr-code-generator.com/*

De posse do comprovante, o voto individual pode ser facilmente auditado pelo próprio eleitor, o que aumenta significativamente a dificuldade de fraudes. Terceiros podem replicar a blockchain utilizada no processo eleitoral e fornecer serviços concorrentes de auditoria dos votos, sem comprometer a confiabilidade do sistema como um todo.

Para evitar que o comprovante sofra danos físicos e tenha o seu valor destruído, uma cópia pode ser enviada por meios digitais ao eleitor, como um e-mail ou SMS, ficando a cargo do eleitor informar em quais meios deseja receber a cópia.

Como o registro dos votos é de domínio público, eleitores fantasmas podem facilmente ser rastreados verificando as contas criadas com a origem das moedas destinadas à votação.

**Figura 3 - Exemplo de uma Árvore de Merkle formada a partir das assinaturas digitais das transações.**




*https://blog.ethereum.org/2015/11/15/merkling-in-ethereum/*

Já a ordem de inserção das transações nos blocos pode ser embaralhada de modo que um terceiro não consiga quebrar o sigilo do voto correlacionando os registros de votação da blockchain com os registros de emissão dos comprovantes de voto.

Utilizando a metodologia de software livre, é possível tornar o código fonte do sistema auditável e replicável para todos os eleitores, sem expor o sistema a riscos. Isso é possível graças à matemática da criptografia dos votos. Se o software da blockchain for alterado, os elos produzidos nas correntes terão valores diferentes dos QRCodes em posse dos eleitores e dos replicados pela rede P2P.

## 7. Conclusão

Utilizando blockchains, QRCodes, carteiras digitais e outras tecnologias presentes nas moedas digitais, é possível criar um processo eleitoral totalmente transparente, seguro, veloz e auditável pela própria população. A matemática e a redundância presente no seu funcionamento garantem a confidencialidade, confiabilidade e integridade do voto e do processo eleitoral de forma nunca antes atingida pela atual urna eletrônica.

O modelo de blockchain a ser adotado deve permitir a alteração dos seus padrões de forma registrada e consensual dos nodos, como o tamanho dos blocos, forma de validação, etc., para permitir que a blockchain utilizada seja escalonável e acompanhe a evolução tecnológica sem perder o seu valor, como ocorre com os forks da rede bitcoin.

Além disso, a própria blockchain pode se tornar um padrão não só de votos, mas de todos os registros digitais em todas as funções do Estado, como cartórios, contratos inteligentes, etc., aumentando ainda mais o volume de dados e a complexidade da blockchain, tornando-a ainda mais segura.

**Referências**


**Voto passará a ser impresso pela urna eletrônica.** Disponível em: https://www.youtube.com/watch?v=h2PIplFL5rM. Acessado em: 23 out. 2017.

**The Future of Democracy | Santiago Siri | TEDxStPeterPort**. Disponível em: https://www.youtube.com/watch?v=yGmGWZCE4h0. Acessado em: 23 out. 2017.

**Democracy Earth Foundation.** Disponível em: http://democracy.earth

**Sessão do Senado, em 2 de setembro de 2015 – PLC 75/2015**. Disponível em: https://www.youtube.com/watch?v=dqRuNckzAnE&t=1214s. Acessado em: 23 out. 2017.

**Bitcoin - Dinheiro P2P de código aberto.** Disponível em: https://bitcoin.org/pt_BR/. Acessado em: 23 out. 2017.

**WTF Is The Blockchain? A Guide for Total Beginners.** Disponível em: http://dataconomy.com/2015/10/wtf-is-the-blockchain-a-guide-for-total-beginners/. Acessado em: 23 out. 2017.

**Internet Voting? Really? | Andrew Appel | TEDxPrincetonU**. Disponível em: bhttps://www.youtube.com/watch?v=abQCqIbBBeM&t=908s. Acessado em: 23 out. 2017.

**Why Electronic Voting is a BAD Idea – Computerphile**. Disponível em: https://www.youtube.com/watch?v=w3_0x6oaDmI. Acessado em: 23 out. 2017.

**Voto impresso começa a valer em 2018, mas já é alvo de críticas.** Disponível em: http://www12.senado.leg.br/noticias/materias/2016/02/23/voto-impresso-comeca-a-valer-em-2018-mas-ja-e-alvo-de-criticas. Acessado em: 23 out. 2017.

**Ataques de malware já afetaram 30% dos internautas brasileiros neste ano.** Disponível em: http://computerworld.com.br/ataques-de-malware-ja-afetaram-30-dos-internautas-brasileiros-neste-ano. Acessado em: 23 out. 2017.

**Proof of Work VS Proof of Stake - A simplified Explanation.** Disponível em: https://www.youtube.com/watch?v=SiKnWBPkQ4I. Acessado em: 23 out. 2017.

**EB58 – Vitalik Buterin: Ethereum, Proof-of-Stake, The Future Of Bitcoin.** Disponível em: https://www.youtube.com/watch?v=qPsCGvXyrP4. Acessado em: 23 out. 2017.

**The Blockchain Explained to Web Developers, Part 1: The Theory.** Disponível em: https://marmelab.com/blog/2016/04/28/blockchain-for-web-developers-the-theory.html. Acessado em: 23 out. 2017.

**Merkling in Ethereum.** Disponível em: https://blog.ethereum.org/2015/11/15/merkling-in-ethereum/. Acessado em: 23 out. 2017.

# Privacidade líquida e incerta

**Gustavo Grossi**

Precisamos falar sobre privacidade. Sim, privacidade. Lembram-se dela? Ao ressuscitar o tema, sei que corro o risco de soar rabugento e anacrônico, num tempo de reality shows, videovigilância, mídias sociais, espetacularização generalizada da intimidade e por aí vai. Mas o ofício desta coluna não é reavivar criticamente a memória de seus leitores?

Convido-os, então, a recuar nossa timeline até janeiro de 2010, quando Mark Zuckerberg declarou a privacidade um valor ultrapassado, quiçá extinto. Na ocasião, Zuckerberg justificava o sentido de alterações na política de privacidade do Facebook, com base em evidências de que a publicidade ascendera ao posto de valor hegemônico na rede. Em resumo, a maioria dos usuários da internet teria decidido, por livre escolha, "curtir" e "compartilhar" os benefícios da publicização de dados privados. Renunciar à privacidade em favor da publicidade e da transparência em rede seria, nessa perspectiva, um sacrifício menor e ine-

Banco de Imagens

vitável, válido pelo usufruto geral dos benefícios da interconexão global.

Dez anos depois dessa declaração, a "nação Face" só fez crescer, alcançando a exponencial marca de 2 bilhões de usuários. Uma nação que gera insumos para os mais diversos índices, alguns deles peculiares. Quer um exemplo? A equipe do Data Science Team do Facebook chegou a conceber um modo de calcular a "Felicidade Interna Bruta" de um país a partir de dados computados pela rede social. Versão alternativa do usual Produto Interno Bruto (PIB), a elaboração do índice utilizou o registro de ocorrências de termos e frases que denotam emoções positivas ou negativas para gerar um modelo estatístico de análise de tendências sociais – a mensuração dos cliques da felicidade.

Com isso em mente, aportemos agora à época e às ideias do filósofo, jurista e reformador social britânico Jeremy Benthan (1748-1832), autor do lema: "A maior felicidade possível para o maior número possível de pessoas". Benthan foi um dos expoentes do utilitarismo, linha de pensamento que busca estabelecer uma espécie de cálculo do bem comum. Ele defendia uma ética de maximização da utilidade e da felicidade como resposta às questões sobre como conduzir a vida em sociedade. Não à toa, críticos das mídias sociais costumam associar os princípios da filosofia utilitarista – a qual não tem a privacidade em grande conta – às ideias professadas por visionários contemporâneos do Vale do Silício e adjacências espirituais, políticas e negociais mundo afora.

Benthan celebrizou-se ainda pela concepção do panóptico, modelo de prisão circular que propiciava ao observador a visualização "transparente" de todos os locais onde estivessem os presos – ou alunos, trabalhadores e pacientes, uma vez que fora projetado para funcionar também em escolas, oficinas e manicômios. Transparência, no caso, implicava racionalização, monitoramento, eficiência, visibilidade e controle, no rastro da disseminação sistemática de dispositivos disciplinares nas instituições da sociedade ocidental.

Pois tais dispositivos prefiguraram novos regimes de visibilidade no decorrer da história. Vide o surgimento de formas sutis e naturalizadas de vigilância, voyeurismo e narcisismo em rede, ligadas ao desenvolvimento das tecnologias da informação e comunicação, em especial a partir da segunda metade do século XX. Daí também as tensões e interesses geopolíticos, econômicos e culturais inerentes à constituição de um ecossistema digital no qual somos, ao mesmo tempo, consumidores e produtores de conteúdos e informações. Juntou-se, portanto, a vontade de ver e (editar-se para) ser visto com a fome de informação, poder e lucro de conglomerados condominiais da internet – nesse processo, o próprio usuário é o produto.

Contudo, nem toda exposição é voluntária. Quando um dispositivo pessoal ou corporativo conecta-se à rede, abrem-se flancos para práticas sub-reptícias de monitoramento, identificação e coleta de informações relativas a indivíduos e organizações. Todos estão interconectados em algum nível, e o que cai na rede torna-se passível de usos e abusos à revelia de seus usuários. Uma condição que, diga-se, não é prerrogativa do espaço virtual.

Com as fronteiras entre o on-line e o of f-line praticamente indistinguíveis, sensores e dispositivos discretos monitoram o chamado espaço físico, de modo a criar uma espécie de realidade ampliada, na qual tudo está imerso e sujeito a algum tipo de registro e vigilância. Se consciência é algo que temos quando as pessoas estão nos olhando, lembrem-se de que hoje elas também nos filmam e podem vazar o arquivo na web. De certa forma, já protagonizamos diariamente enredos típicos da série britânica Black Mirror, os quais projetam, num futuro próximo, situações perturbadoras acerca de nossa relação com a tecnologia.

Para encerrar esta minha cantilena, cabe perguntar: afinal, a privacidade está de fato sendo imolada no altar da publicidade?

A concepção de privacidade não é um dado fixo da realidade, uma condição "natural" sujeita a um princípio evolutivo que levaria à sua substituição pela publicidade. As apreciações em torno dela giram em torno da atribuição de valor e da disputa pelo sentido de uma categoria social sujeita a variações históricas. E o modo como compreendemos a privacidade resultou de tensões e conflitos que deixaram marcas civilizatórias, tais como a separação entre o público e o privado e a valorização dos direitos do indivíduo. Ocorre que, hoje, numa analogia com as formulações do sociólogo polonês Zygmunt Bauman (1925-2017), experimenta-se uma espécie de "privacidade líquida", em meio à diluição que põe em xeque os limites do público e do privado.

Portanto, é bom desconfiar quando representantes de conglomerados de mídia social anunciam de modo taxativo o fim da privacidade, pois o diagnóstico coincide com modelos de negócio e interesses estratégicos a que estão ligados. A esse respeito, a pesquisadora Fernanda Bruno faz uma observação bastante perspicaz: não são as empresas que bradam pela redução da privacidade as mesmas que reivindicam com fervor a própria privacidade se questionadas sobre os usos da massa de dados pessoais que capturam de seus usuários?

# Educação a Distância Prodemge.

## Economia e flexibilidade na disseminação do conhecimento.

**Tendência em todo o mundo, a educação a distância é a melhor maneira de capacitar os colaboradores das instituições. Acreditando nisso, a Prodemge trouxe essa modalidade para as entidades da administração pública em Minas Gerais.**

**Por meio de cartoons, videoaulas, cursos, games, tutoriais ou storytelling, a Educação a Distância da Prodemge proporciona às instituições:**

- redução dos custos com capacitação, considerando inclusive os custos com deslocamentos;
- aumento do grupo de pessoal capacitado;
- disponibilização do conteúdo para consultas posteriores;
- atualização do conteúdo de acordo com alterações necessárias.

Acesse **www.prodemge.gov.br** e veja como a Prodemge pode desenvolver a melhor solução para a necessidade da sua instituição.

50 ANOS | prodemge |

MINAS GERAIS
DIÁLOGO EQUILÍBRIO TRABALHO

# Quando o assunto é segurança na rede, o caminho certo é o Certificado Digital Prodemge.

Conte com quem entende de tecnologia para realizar transações e serviços eletrônicos com segurança.

Com preços competitivos e diversos postos de atendimento, a Prodemge oferece suporte técnico e serviço de excelência*.

Entre para o **#mundovirtualseguro**.

** 97,7 % dos clientes satisfeitos*

/certificadodigitalprodemge

@prodemge

Para mais informações, acesse o site
http://www.prodemge.gov.br/certificacaodigital
ou entre em contato com o suporte
atendimento.cd@prodemge.gov.br
Tel. (31) 3339-1251

CERTIFICADO DIGITAL PRODEMGE