# Saiba o que seus arquivos corporativos dizem sobre sua estratégia de segurança

Carlos Rodrigues (*)

*Os gastos com segurança digital vêm crescendo de maneira constante nos últimos anos, e devem alcançar quase US$ 100 bilhões em todo o mundo em 2018, de acordo com informações do Gartner*

No entanto, se engana quem pensa que, de alguma maneira, isso pode levar a uma redução no número de incidentes de segurança reportados.

Dados divulgados pelo CERT.br revelaram que, nos últimos dois anos, o número de incidentes cresceu vertiginosamente. Em 2017, foram reportados mais de 833 mil incidentes – são praticamente mais de 2 mil incidentes por ano. A tendência é que, em 2018, esse número seja ainda maior com a aplicação de novos ataques tirando proveito de eventos mundiais, como a Copa, causando disrupções massivas e custosas em escala global.

Novas regulamentações, como o GDPR, que passou a valer na Europa e deve afetar empresas em todo o mundo que lidam com dados de cidadãos europeus e vai exigir que as empresas monitorem e reportem violações de dados, estão pressionando os executivos brasileiros para investir cada vez mais na segurança das informações.

Diante deste cenário, o Varonis Global Data Risk Report chamou a atenção para a quantidade de dados sensíveis abertos a todos os funcionários nas empresas, revelando que, em média, 21% das pastas nas organizações estão acessíveis a todos os colaboradores, e 41% das organizações tinham, ao menos, 1.000 arquivos sensíveis abertos a todos os funcionários – incluindo dados sensíveis regulados pelo PCI-DSS, pelo GDPR e outros padrões. Essa é apenas uma das descobertas que podemos fazer quando damos atenção aos dados ocultos nos sistemas corporativos.

Com o volume crescente de informações que temos produzido, a tendência é que os ataques, sejam eles de origem interna ou externa, sejam cada vez mais destrutivos – bem mais do que precisam ser.

**Você pode não saber onde estão seus dados, mas os hackers sabem**

É fácil demais para as ameaças internas e externas (que já estão dentro da rede) terem acesso às suas informações mais valiosas. No caso das ameaças internas, como já têm acesso aos dados, tudo o que precisam fazer é bisbilhotar para encontrar os arquivos desprotegidos.

Já no caso dos hackers externos, basta penetrar as defesas do perímetro da rede – algo que é feito com facilidade, especialmente pelos cibercriminosos mais sofisticados. As portas de entrada favoritas são os e-mails de phishing, que, depois de fazerem as vítimas baixar os malwares, dão aos hackers acesso efetivo aos recursos internos, como se fossem funcionários.

Além do phishing, os hackers também se aproveitam de vulnerabilidades como senhas fracas e falhas de segurança em sistemas desatualizados. Por isso, muito além de investir em soluções pontuais, é fundamental estar atento ao que acontece com o que de fato deve ser protegido: suas informações.

Infelizmente, a maioria das empresas não sabe o que se passa dentro do perímetro. Nas conversas que temos com executivos de tecnologia da informação e líderes de segurança digital, fazemos sempre o mesmo tipo de pergunta: "Como você saberia se 10 mil dos seus arquivos contendo dados sensíveis estivessem corrompidos ou fossem acessados ou deletados?".

A resposta pode ser surpreendente para quem nunca trabalhou com TI, mas a maioria das organizações não está monitorando o modo como seus arquivos são usados. Sem esse monitoramento, é muito difícil detectar quando os dados estão em perigo. Imagine, por exemplo, que uma empresa de cartões de crédito esteja tentando detectar transações fraudulentas sem conseguir monitorar as cobranças – é praticamente impossível.

**Invista seus recursos onde os riscos estão**

Na medida em que o volume de dados cresce, as empresas que investirem de maneira inteligente, com base na priorização dos riscos, vão estar muito melhor preparadas para a próxima onda de ciberataques do que aqueles que decidiram ficar no escuro em relação aos seus dados.

Se sua empresa é uma das que pretendem aumentar os investimentos em segurança, elaboramos alguns passos que vão ajudá-lo a garantir um alto retorno de investimento:

**1. Avalie seus riscos**

Identifique dados importantes, sensíveis e regulados onde provavelmente estão e, ainda mais importante: onde você menos espera que estejam. Vá além, e mapeie quem tem acesso a essas informações, monitorando se estão sendo usadas (ou não) e por quem. Isso vai ajudá-lo a decidir se todos os dados que você tem são necessários ou não (é provável que metade deles esteja obsoleta), para ver onde estão mais expostos e sujeitos a ameaças.

**2. Comece a lidar com os riscos**

Depois de identificar onde estão seus dados sensíveis, como os dados de cartões de crédito e as informações pessoais de clientes e funcionários, comece a isolá-los e tornar seu acesso mais difícil para funcionários com credenciais de segurança comuns e hackers. Além disso, arquive, delete ou coloque em quarentena os dados desnecessários – essas informações são pouco benéficas para você e muito vantajosas para os cibercriminosos.

**3. Minimize os riscos**

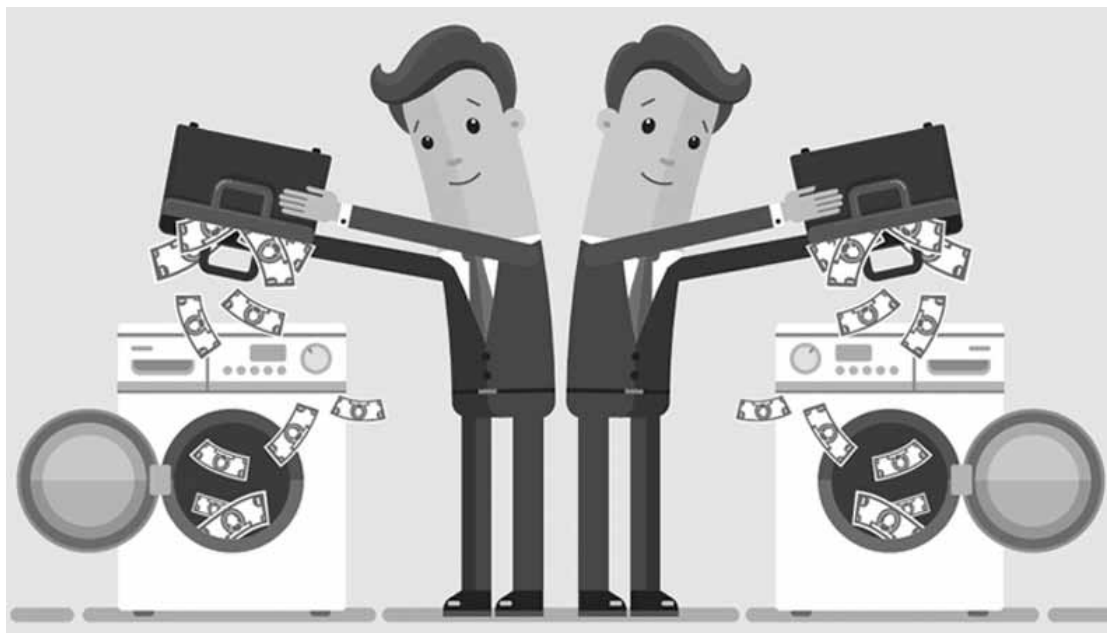
Defina proprietários de dados para tomar decisões importantes relacionadas às informações: quem deve ganhar ou perder acesso? O que pode ser considerado um uso aceitável da informação? Quando um dado deve ser deletado? Depois disso, ajude-os a tomarem decisões com o mínimo de esforço manual. Com isso, você reduz os riscos e aumenta a eficiência ao mesmo tempo.

**(*) É vice-presidente da Varonis para a América Latina.**

# Prevenção à lavagem de dinheiro – as empresas devem fazer a sua parte

Nos últimos anos, o brasileiro passou a conviver diariamente com notícias sobre a corrupção nos mais diversos níveis dentro e fora de todas as esferas dos governos federal, estaduais e municipais

**Juliana Ribeiro Soares (*)**



O que deveria ser algo extremamente isolado virou uma prática corriqueira e até usual para muita gente que deveria ser modelo de lisura e de caráter ilibado.

Dentre os mais variados tipos de corrupção, um é tema recorrente nos noticiários: a lavagem de dinheiro. Mas, o que realmente significa esta expressão?

Trata-se do procedimento usado para disfarçar a origem de recursos ilegais. É quando alguém ganha dinheiro de forma ilícita e não pode sair por aí gastando o que "conquistou". E, para tentar esconder os indícios de que fez algo errado, arma estratégias para afastar toda e qualquer suspeita dos órgãos competentes pelas investigações.

O termo surgiu nos Estados Unidos para mascarar um tipo de falsificação de dólares. Os fraudadores colocavam as notas em uma máquina de lavar para que elas ficassem com uma aparência bastante usada. Mas, com o passar dos anos, o método mudou (e muito).

A integração do sistema financeiro mundial tem permitido que os recursos passem de uma conta bancária para outra, de um país para o outro, tudo em questão de segundos. Assim, o "dinheiro sujo" acaba sendo incorporado à economia.

Segundo estimativas do Fundo Monetário Internacional (FMI), de 2,5% a 5% do Produto Interno Bruto (PIB) de cada país no mundo têm origem ilícita. Em termos de Brasil, apenas para citar um exemplo, esse percentual equivaleria de R$ 165 bilhões a R$ 330 bilhões (PIB do Brasil em 2017 = R$ 6,6 trilhões).

Mas, engana-se quem acha que a lavagem de dinheiro está restrita apenas aos governos. Infelizmente, ela também está presente dentro das empresas. Neste contexto, para ajudar a combater tal problema, o Brasil aprovou, em março de 1998, a Lei nº 9613, que dispôs sobre os crimes de lavagem ou ocultação de bens, direitos e valores; a prevenção da utilização do sistema financeiro para os ilícitos previstos nesta Lei; criou o Conselho de Controle de Atividades Financeiras (COAF) e deu outras providências ao tema.

Esta Lei atribuiu às pessoas físicas e jurídicas, de diversos setores econômico-financeiros, uma maior responsabilidade na identificação de quem pode ter dinheiro ilícito, com a manutenção de registros de todas as movimentações e com a comunicação de operações suspeitas. Foi uma forma de dar continuidade a compromissos internacionais assumidos a partir da assinatura da Convenção de Viena, de 1988.

Em relação ao COAF, para quem não sabe, é o órgão responsável por receber, examinar e identificar as ocorrências suspeitas de atividades ilícitas e também por comunicar às autoridades competentes para a instauração dos procedimentos cabíveis. Além disso, coordena e propõe mecanismos de cooperação e de troca de informações que possam ajudar a viabilizar o combate à ocultação ou dissimulação de bens, direitos e valores; disciplina e aplica penas administrativas; e assessora os setores econômicos para os quais não haja instituição reguladora ou fiscalizador próprio.

E para ajudar a combater esta prática desonesta, tem sido cada vez maior o número de empresas nacionais que começaram a implantar, em sua rotina de Compliance, o processo de Prevenção à Lavagem de Dinheiro (PLD), um programa para impedir que isto ocorra dentro do ambiente corporativo.

No entanto, para que a PLD seja de fato efetiva, é preciso que todos os colaboradores tenham conhecimento sobre o que é o programa, e como ele funciona dentro da organização, para estarem envolvidos na inibição a este tipo de crime. É preciso criar uma cultura de buscar informações e verificar, sempre, empresas e pessoas relacionadas ao negócio, e, sobretudo, analisar a fundo o universo o qual está inserido.

Por isso, é indiscutível a importância de implementar – e conscientizar-se sobre – o programa de Prevenção à Lavagem de Dinheiro. Afinal, só assim será possível ter base e, principalmente, plena ciência dos fatos para tomar decisões assertivas para combater os delitos desta natureza.

**(*) É gerente de Compliance do pag!**

# Blockchain: como implementar do campo à mesa do consumidor?

A internet é, sem dúvida, a base do movimento de inovação. Da mesma forma que os custos de comunicação da internet caíram para valores próximos a zero, espera-se que os custos transacionais e organizacionais também caiam próximos a zero, à medida que estruturas organizacionais estão sendo, cada vez mais, distribuídas e habilitadas para informação.[1]

Logo, é nesse movimento que a tecnologia Blockchain vem agregando valor a diversos modelos de negócios para reduzir custos de transações e torná-las auditáveis, gerando confiança. O setor de agronegócios, por exemplo, pode aproveitar novas oportunidades em tecnologia, diante das diversas soluções a serem exploradas, uma vez que é tradicionalmente muito conservador.

O Brasil, que é o maior país da América do Sul e da região da América Latina, sendo o quinto maior do mundo em área territorial, com 8.516.000 km², pode, por exemplo, romper essa barreira geográfica com a tecnologia Blockchain, aliada à Computação Cognitiva e Internet das Coisas, possibilitando maior assertividade para agilizar toda cadeia de produção de um produto, com dados registrados à prova de fraudes. Quando se fala em produtos perecíveis, a referida assertividade é primordial, uma vez que, através da tecnologia, repensa-se todo o design organizacional existente para redução do tempo de logística e fraude, economizando, muito provavelmente, valores consideráveis para esse mercado.

Para exemplificar os benefícios mencionados, seja pela tecnologia Blockchain ou por redes permissionadas, em outubro de 2016, a empresa Maersk participou da criação do protótipo do projeto de digitalização do fluxo de trabalho no transporte, em parceria com a IBM, eliminando documentos em papel, que pode substituir a documentação tradicional. Sua demonstração foi realizada na entrega de recipientes com flores frescas do Quênia para o porto de Roterdã. Além disso, esquemas semelhantes foram testados no fornecimento de lotes de laranja na Califórnia e abacaxi da Colômbia.

Não é à toa que, no Brasil, a IBM pesquisa soluções digitais com Blockchain voltadas ao agronegócio. Em 2017, a IBM Brasil[2] anunciou o desenvolvimento da plataforma IBM AgriTech, em parceria com empresas tradicionais do agronegócio e com companhias emergentes do setor de tecnologia agrícola brasileiro, para consolidar dados, tecnologias e soluções capazes de resolver as demandas daquele mercado.

Assim, empresas que já são globais e integradas podem tornar-se ainda mais rápidas em suas transações negociais, aumentando a capacidade de competição, maior expansão, mas com um sistema de troca segura de dados para certificar toda complexidade e volume de informações que o mercado de agronegócio exige. A possibilidade, portanto, de que dados auto executáveis, programados numa tecnologia que torne os registros imutáveis, auxiliem esse mercado, refere-se tanto pela imprescindibilidade de exportação, como pela necessidade de garantir, de forma sustentável, o transporte, armazenamento e entrega dos produtos que irão do campo à mesa do consumidor.

É nessa lógica de integração de troca segura de dados que se reflete sobre diversas implementações para o agronegócio, com a junção de computação cognitiva, IoT e Blockchain, desde aplicação em títulos de crédito, como a Cédula e Nota de Crédito Rural, relacionadas ao financiamento das atividades agrícolas e agropecuárias, até transporte de cargas fracionadas. Vislumbra-se, portanto, maior sofisticação da cadeia global de alimentos e do agronegócio, com maior integridade das informações, reduzindo fraudes, custos e tempo despendido.

**(Fonte: Amanda Lima é articulista do Manual Bockchain).**

## News @TI

### Brasil melhora cinco posições no Índice Global de Inovação e chega ao 64º lugar

@O Brasil ganhou cinco posições no Índice Global de Inovação (IGI) deste ano, subindo do 69º para o 64º lugar em um ranking de 126 países. No entanto, o avanço não coloca o país na liderança da inovação na América Latina, que segue com o Chile na primeira posição regional. A classificação é publicada anualmente pela Universidade Cornell, pelo INSEAD e pela Organização Mundial da Propriedade Intelectual (OMPI). A Confederação Nacional da Indústria (CNI) e o Serviço Brasileiro de Apoio às Micro e Pequenas Empresas (Sebrae) são parceiros do IGI (https://www.globalinnovationindex.org/Home).