TESTE DE DETECÇÃO DE VULNERABILIDADES COMO FERRAMENTA DE SEGURANÇA DAS INSTITUÇÕES FINANCEIRAS [1]

Ethienne Chaves West

Resumo: O artigo procurou discutir o cenário no qual as instituições financeiras brasileiras se valem de testes de detecção de vulnerabilidades para compor seu portfólio de ferramentas utilizadas na gestão de risco de segurança da informação. Na fase de avaliação de risco, o teste de segurança é uma ferramenta importante, pois oferece subsídios para identificação e, consequentemente, mitigação dos riscos envolvidos com as vulnerabilidades encontradas. Os testes, além de serem componentes gerenciais da administração do risco, também são uma exigência do Banco Central do Brasil e de outros reguladores, devendo ser um dos procedimentos mínimos adotados para compor a política de segurança cibernética das instituições. Dada a relevância dos testes de detecção, propôs-se, neste artigo, a implementação de uma agenda de testes para as empresas, que consiste em pelo menos um teste anual de penetração e dois testes de avaliação de vulnerabilidades.

Palavras-chave: Teste. Risco. Instituições. Financeiras.

1 INTRODUÇÃO

Este artigo foi construído inicialmente com a intenção de explorar a relação das instituições financeiras com os preceitos da gestão de risco de segurança da informação. Isto porque, o setor financeiro tem suas peculiaridades no que diz respeito à segurança da informação. De um lado, temos o cenário atual, com clientes mais informados e exigentes em relação a novas tecnologias que venham a melhorar a experiência do usuário. De outro, tem-se as instituições financeiras, que manipulam, a todo o tempo, informações sensíveis, tanto as suas próprias como as de terceiros.

Essa dicotomia entre a necessidade constante de modernização e o acesso a informações sigilosas pode ser um dos motivos pelo qual as instituições financeiras investem tanto em tecnologia. Segundo dados da Federação Brasileira de Bancos (FEBRABAN, 2018), o valor gasto pelas instituições financeiras em tecnologia no

[1] Artigo apresentado como Trabalho de Conclusão do Curso de Especialização em Gestão de Segurança da Informação, da Universidade do Sul de Santa Catarina, como requisito parcial para a obtenção do título de Especialista em Gestão de Segurança da Informação.

Brasil somou R$ 19,5 bilhões em 2017, um aumento de 5 % em relação a 2016. Mas a ampla oferta de novas tecnologias abre o leque de ameaças às quais os bancos estão suscetíveis, e proteger os ativos, nesse caso, particularmente, a informação, é crucial para a manutenção do negócio. Uma estimativa do Fundo Monetário Internacional aponta que o risco de perdas causadas por ataques cibernéticos pode variar entre 9 % do resultado líquido à metade dos lucros, no setor bancário (Lagarde, 2018), ou seja, dependendo da magnitude do ataque, ele pode levar uma instituição à insolvência.

Os dados apontados no parágrafo anterior são apenas alguns exemplos que procuraram ilustrar como a preocupação com a segurança da informação e o gerenciamento do risco deve ser uma prioridade dentro do setor financeiro. Verificou-se inclusive que o Banco Central do Brasil (BACEN), em sua Resolução 4.658, reconhece a importância dessas questões ao exigir das instituições financeiras a implantação de uma política de segurança cibernética. Nela, deve constar, entre outras coisas, um cronograma de testes de detecção de vulnerabilidades.

Ao procurar identificar as ferramentas à disposição das instituições financeiras que poderiam auxiliá-las na mitigação dos riscos envolvidos com a alta informatização dos sistemas que compõem a vasta gama de soluções oferecidas pelos bancos, novamente deparou-se com o teste de detecção de vulnerabilidades. Observou-se que esta é uma ferramenta versátil, que pode testar diferentes tipos de sistema e aplicações, dependendo da necessidade e do intuito da instituição.

Portanto, dada a relevância do assunto, este artigo procurou fazer um levantamento sobre a necessidade da realização de testes de detecção de vulnerabilidades nas instituições financeiras brasileiras, bem como sua importância no contexto da gestão de risco de segurança da informação. Para isto, fez-se necessário:

- Discorrer sobre a Resolução nº 4.658, de 24/06/2018, do Banco Central do Brasil (BACEN);

- Pesquisar sobre os testes de detecção de vulnerabilidades: tipos, métodos, necessidade e aplicação;

- Dissertar sobre a gestão de risco voltada para a área de segurança da informação;

- Correlacionar os testes de detecção de vulnerabilidades à busca pela mitigação do risco.

Dado o caráter conceitual do tema do artigo, que pretendeu buscar conhecimento na literatura sobre a importância dos testes de detecção de vulnerabilidades para as instituições financeiras no contexto da gestão de risco, a pesquisa foi pura (fundamental).

Por consequência, a produção do conhecimento foi realizada por meio de pesquisa teórica. Assim, após a coleta das informações bibliográficas disponíveis sobre o tema, a pesquisa buscou correlacionar essas informações de modo a explicar a importância dos testes de detecção de vulnerabilidade para as empresas da área financeira levando-se em conta aspectos gerenciais, estratégicos e de conformidade (pesquisa explicativa).

Na seção 2, é feita uma pequena introdução sobre o Banco Central do Brasil, suas atribuições e sua Resolução nº 4.658, que dispõe sobre as políticas de segurança cibernética. Na seção 3, são apresentados os conceitos relacionados à gestão de risco de segurança da informação, principalmente aqueles relacionados à avaliação de risco. Na seção 4, discorre-se sobre o aspecto mais teórico dos testes de detecção de vulnerabilidades, como tipos, métodos, etc. e também sobre um modelo de implementação de política relacionada a esses testes. E, finalmente, na seção 5, são apresentadas as conclusões do artigo.

2 BANCO CENTRAL DO BRASIL

O Banco Central do Brasil (BACEN) é uma autarquia federal, vinculada ao Ministério da Fazenda, que tem, entre suas atribuições, exercer a fiscalização das instituições financeiras. O Banco Central é o órgão responsável por fazer a regulação e supervisão dos bancos no Brasil (BACEN, 2018).

2.1 Resolução BACEN 4.658

A ideia inicial para confecção deste artigo surgiu com a divulgação da Resolução nº 4.658, de 24/06/2018, do BACEN. Em sua ementa, está transcrito o seguinte:

> Dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil.

Pode-se dizer que esse é um marco regulatório no que diz respeito à cibersegurança bancária. Com esta Resolução, o BACEN reconhece a importância da implantação de uma política de segurança cibernética séria para a manutenção das instituições financeiras brasileiras.

Segundo pesquisa realizada pela Associação Brasileira das Entidades dos Mercados Financeiros e de Capitais, 29 % das instituições financeiras brasileiras entrevistadas não possuem um programa formal de segurança cibernética (ANBIMA, 2018). Ou seja, segundo a Resolução 4.658 e o disposto em seu Art. 26, estas empresas têm até o dia 6 de maio de 2019 para ter uma política de segurança cibernética aprovada pelo seu conselho de administração ou, na sua inexistência, pela diretoria da instituição (Art. 9º).

Este é um dado preocupante, não somente pelo aspecto da obrigatoriedade legal, mas também pela importância de se manter uma política de segurança que englobe também a cibersegurança, pois a política é o instrumento que fornece à empresa orientação em relação à gestão da segurança da informação, na forma de diretrizes, normas, procedimentos e instruções. Seu caráter oficial garante o comprometimento e o envolvimento da alta direção, que é compartilhado posteriormente com todos os funcionários da organização (Sêmola, 2003).

Ao deixar a parte gerencial de lado no momento para retornar ao aspecto regulamentar do tema em questão, o ponto central a ser ressaltado na Resolução 4.658, diz respeito ao seu Art. 3º, inciso II, que estabelece que “a política de segurança cibernética deve contemplar, no mínimo (...) os procedimentos e os controles adotados para reduzir a vulnerabilidade da instituição a incidentes”. Os mesmos devem abranger, de acordo com o § 2º,

> ..., no mínimo, a autenticação, a criptografia, a prevenção e a detecção de intrusão, a prevenção de vazamento de informações, a realização periódica de testes e varreduras para detecção de vulnerabilidades, a proteção contra softwares maliciosos, o estabelecimento de mecanismos de rastreabilidade, os controles de acesso e de segmentação da rede de computadores e a manutenção de cópias de segurança dos dados e das informações.

Isto coloca, portanto, os testes de detecção em pé de igualdade com outras formas mais conhecidas e estabelecidas de controle e prevenção de risco, como a criptografia e o controle de acesso. Ora, se o órgão responsável pela regulação e supervisão do Sistema Financeiro Nacional (SFN) determina que sejam realizados testes de vulnerabilidade periodicamente, fica notória a importância destes testes para as instituições financeiras brasileiras. Mas é preciso levar a discussão para além do aspecto da obrigatoriedade legal. Claramente, as instituições financeiras deverão incluir os testes de detecção de vulnerabilidades em seus cronogramas, mas é certo que a atividade seria mais proveitosa se fosse realizada não somente para cumprir a determinação do BACEN, mas principalmente como forma de auxiliar essas empresas na detecção e, consequentemente, no controle de suas vulnerabilidades.

3 GESTÃO DE RISCO DE SEGURANÇA DA INFORMAÇÃO

As vulnerabilidades estão diretamente ligadas ao risco. Segundo Sêmola (2003), risco é a "probabilidade de ameaças explorarem vulnerabilidades, provocando perdas de confidencialidade, integridade e disponibilidade, causando, possivelmente, impactos nos negócios". De uma maneira mais holística, a ISO 31000 (2018) define risco como sendo incidência de incerteza nos objetivos. Mas, independente da abrangência do conceito, fato é que o risco é inerente a qualquer organização, pois suas atividades estão cercadas por algum grau de incerteza, já que envolvem elementos como pessoas, sistemas, mercado e diversas outras variáveis que podem exercer influência sobre o negócio.

A maneira como uma organização responde ao risco reflete o valor que ela atribui a seus próprios ativos (KIM; SOLOMON, 2014). Uma empresa que enxerga seus ativos como elementos indispensáveis para a manutenção do negócio no longo prazo tende a investir na proteção destes ativos e, após a identificação dos riscos que podem vir a ameaça-los, a organização pode escolher lidar com eles de uma dessas três

formas: aceitar, mitigar ou eliminar e transferir (na forma de um seguro, por exemplo); e é assim, em linhas gerais, como gerenciamos o risco (Northcutt, 2000, p.208).

O ideal seria que todo o risco fosse eliminado, mas isso não é possível, dada a imprevisibilidade de sua natureza. Outra questão a ser levada em consideração é o custo: um negócio rentável deve estar disposto a aceitar algum grau de risco. Segundo Sêmola (2003), o impacto do risco sobre o negócio é inversamente proporcional às medidas de segurança aplicadas para proteção de seus ativos.

No entanto, não se pode, por exemplo, investir um valor maior na segurança de um ativo do que o valor que ele tem ou gera para a empresa. Portanto, uma organização deve buscar o equilíbrio entre um nível aceitável de risco e o custo para reduzi-lo (KIM; SOLOMON, 2014), lembrando que a tolerância ao risco difere entre organizações, dependendo do seu negócio, a criticidade das informações que elas manipulam, o mercado onde estão inseridas, etc. Além disso, reavaliações periódicas devem ser feitas para identificar novos riscos, bem como mensurar novamente ativos, vulnerabilidades e ameaças (KIM; SOLOMON, 2014). Um ativo com risco alto devido ao seu valor estratégico para a empresa pode perder valor com o tempo, tornar-se obsoleto, ou até ter seu valor aumentado, o que justificaria maior investimento em segurança para a proteção deste ativo.

Todas essas questões e elementos interferem no risco e devem ser levantados durante o processo de gerenciamento do risco. De acordo com a ISO 31000 (2018), a administração do risco é definida como sendo atividades coordenadas com o intuito de dirigir e controlar uma organização no que tange ao risco. Ou seja, a gestão do risco de segurança da informação é um processo gerencial que auxilia as empresas a identificar, avaliar e medir os riscos de modo a reduzi-lo a um nível aceitável. Portanto, o que se espera da gestão do risco é que ela prepare a empresa para o advento de situações inesperadas que possam vir a comprometer seu negócio.

Segundo Kim e Solomon (2014), gerenciamento de risco é um processo cíclico contínuo que inclui 3 fases:

- estimativa de risco: identificação de riscos, avaliação de riscos, impacto de risco e recomendação de medidas de redução de riscos;

- atenuação de riscos: impedimento de risco, redução de risco, transferência de risco, aceitação de risco e avaliação de riscos;

- avaliação e seguro: estimativa contínua de risco, avaliação periódica e conformidade regulamentar.

3.1 A Avaliação do Risco

Uma das etapas mais importantes do processo de gestão de risco é a avaliação do risco. Para o NIST (2012, capítulo 1, p. 1),

> O propósito das avaliações de risco é informar os tomadores de decisão e dar suporte às respostas ao risco através da identificação de: (i) ameaças relevante às organizações ou ameaças direcionadas a organizações contra outras organizações; (ii) vulnerabilidades de caráter tanto interno quanto externo às organizações; (iii) impacto (isto é, dano) às organizações que pode ocorrer dado o potencial das ameaças que exploram vulnerabilidades; e (iv) a probabilidade que o dano irá ocorrer.

Sêmola (2003, p.48) conceitua vulnerabilidade como sendo uma "fragilidade presente ou associada a ativos que manipulam e/ou processam informações que, ao ser explorada por ameaças, permite a ocorrência de um incidente de segurança". Para que a instituição consiga, por meio da avaliação do risco, identificar suas vulnerabilidades e avaliar o risco dessas vulnerabilidades para o negócio, ela lança mão das mais variadas formas de recurso (humano, técnico, computacional, etc). Segundo a ISO/IEC 31010:2009, "os riscos podem ser avaliados em nível organizacional, departamental, para projetos, atividades individuais ou riscos específicos. Diferentes ferramentas e técnicas podem ser apropriadas em diferentes contextos". No entanto, se o escopo da avaliação for restringido a riscos referentes à segurança da informação no ambiente computacional da organização, o teste de detecção de vulnerabilidades é uma das ferramentas utilizadas para fazer a identificação dessas vulnerabilidades dentro dos sistemas.

4 TESTES DE DETECÇÃO DE VULNERABILIDADES

Segundo Kim e Solomon (2014), a principal finalidade de qualquer teste de segurança é identificar vulnerabilidades não corrigidas em um sistema. Como já foi

dito, vulnerabilidade é uma fragilidade presente ou associada a um determinado ativo e, por ser um elemento passivo, não provoca incidentes por si só (Sêmola, 2003). Ou seja, para que uma vulnerabilidade seja danosa para uma organização, ela necessita ser explorada por um agente ou exposta a alguma situação que culmine em um incidente.

O anonimato, a capacidade computacional crescente e as técnicas de roubo de dados cada vez mais difundidas são alguns dos incentivos que levam criminosos a praticar fraudes eletrônicas. Um relatório elaborado pela Norton (2018) apontou que 62 milhões de brasileiros foram vítimas de crimes cibernéticos, somando uma perda de 22,5 milhões de dólares no ano de 2017.

Nesse contexto, é imperativo que as organizações se municiem de ferramentas que venham a proteger seus ativos de ataques cibernéticos. Uma das ferramentas disponíveis é o teste de detecção, que expõem as vulnerabilidades de um sistema de modo a serem corrigidas antes de serem exploradas por pessoas mal intencionadas.

Dentro da literatura, os testes de detecção de vulnerabilidades aparecem com os mais diferentes nomes: teste de invasão, teste de penetração, teste de intrusão, etc. Para fins de padronização, serão definidos dois tipos de testes, conforme Kim e Solomon (2014):

- Teste de vulnerabilidade: pretende descobrir as falhas em um sistema e determinar quais locais podem ser pontos de ataque;

- Teste de penetração: pretende explorar uma falha no sistema e provar que ele pode ser invadido com sucesso.

Antes do teste em si, para que haja um reconhecimento da estrutura computacional da organização a ser testada, é necessário que se faça o mapeamento da rede, que é quando são descobertos detalhes como endereços de computadores e serviços disponíveis. Esse mapeamento pode vir a permitir a identificação de sistemas, aplicativos, serviços e configurações da rede, facilitando a busca por vulnerabilidades. Entre as técnicas utilizadas para o mapeamento, podemos citar o WHOIS (utilizado para consulta de informações de contato e DNS de empresas na internet), pacotes ICMP ou ping (utilizado para descobrir o esquema de uma rede), NMAP (faz o mapeamento de

portas), etc (KIM; SOLOMON, 2014). Desta forma, os testes terão uma abrangência mais completa, aumentando sua eficácia.

Os testes também podem ser divididos em métodos, dependendo da vulnerabilidade que se queira encontrar. Segundo Kim e Solomon (2014), existem 3 métodos de teste:

- teste de caixa-branca: são feitos a partir do conhecimento do código-fonte da aplicação, visando sua construção;

- teste de caixa-preta: o testador não possui o código-fonte da aplicação, realizando o teste com foco no comportamento externamente visível do software;

- teste de caixa-cinza: o testador tem alguma informação sobre o código-fonte ou tem acesso a documentos com detalhes da arquitetura, por exemplo.

Outra diferenciação importante entre os testes é que eles podem ser feitos em ambiente interno, ou seja, o analista executa o teste dentro da própria empresa-alvo, ou em ambiente externo, quando o teste é realizado fora da empresa-alvo, simulando acessos externos ao ambiente corporativo (Sêmola, 2003). Os testes internos podem ser executados pela própria equipe de TI da empresa, dependendo da capacidade técnica e do nível de acesso a informações sensíveis, mas testadores podem incluir empresas especializadas, auditorias externas ou uma equipe de auditoria interna. O importante é que exista um plano de testes bem definido. O teste deve ser planejado e executado de modo a não ferir aspectos de segurança e evitar indisponibilidades nos serviços. Testes muito invasivos ou executados em horários de pico, por exemplo, podem derrubar sistemas, o que pode gerar grandes prejuízos ao negócio.

4.1 A implementação de uma política de testes de detecção de vulnerabilidades

Após tudo que foi discutido nos parágrafos anteriores, fica evidente a necessidade de as instituições financeiras incluírem testes de detecção de vulnerabilidades em sua política de segurança. No entanto, não está claro como ele deve ser implantado como procedimento periódico e obrigatório dentro do processo de Avaliação do Risco.

O BACEN, em sua Resolução nº 4.658, por exemplo, não especifica tipo ou quantidade de testes a serem realizados, deixando as instituições financeiras sem um modelo de cronograma a seguir. Claro, os testes de detecção de vulnerabilidades podem e devem ser realizados toda vez que uma organização sentir necessidade, baseada sempre em seu compromisso com a segurança da informação, tanto de clientes quanto de parceiros comerciais, funcionários, etc. No entanto, é necessária a criação de uma agenda mínima de testes que venha a constar da política de gestão de segurança, no intuito de validar o comprometimento da organização com o planejamento e gestão do risco.

Neste contexto e baseado no que foi dito até agora, este artigo propõe um cronograma de testes, utilizando como base o modelo estabelecido pelo regulador norte-americano New York State Department of Financial Services, que exige das instituições financeiras que operam em seu território a criação de um programa voltado ao risco e à cibersegurança (NYSDFS, 2018). Este departamento determina, entre outras coisas, que sejam feitos:

- um teste de penetração anual em todos os sistemas informatizados da instituição;

- avaliações de vulnerabilidades bianuais, incluindo varreduras ou revisões nos sistemas informatizados de modo a identificar vulnerabilidades publicamente conhecidas.

Assim, propõe-se que as instituições financeiras brasileiras realizem pelo menos um teste de penetração por ano, que é o teste externo mais abrangente e deve ser realizado em toda a rede da instituição. Sugere-se que seja feita por uma empresa especializada, de modo a garantir que o teste imite da forma mais fiel possível um ataque real. Isto procura assegurar que a empresa tenha a real noção de suas vulnerabilidades, sem a interferência de agentes internos. Essa interferência deve existir somente se houver indisponibilidade do sistema. Devido seu caráter invasivo, a empresa deve planejar o teste cuidadosamente, para garantir que o mesmo seja realizado em dia e hora de pouco impacto ao negócio e quando a equipe de resposta a incidentes esteja preparada para intervir prontamente em caso de indisponibilidades.

As varreduras bianuais podem ser executadas por empresa especializada ou por equipe designada pela área de segurança da própria instituição. Como o teste de

penetração já cobre o ambiente externo de segurança, podem-se realizar testes do tipo interno nesta fase, mas é importante que os funcionários que realizarão os testes não sejam os mesmos envolvidos com o desenvolvimento dos aplicativos, a manutenção da infraestrutura da rede, etc., para que não haja conflito entre a posição de técnico e fiscalizador. O modelo de teste caixa-preta pode ser utilizado para complementar a atividade de varredura.

Além desses dois testes propostos, neste artigo sugere-se ainda que ferramentas para testes caixa-branca sejam disponibilizadas à equipe de construção. Dessa forma, todas as aplicações desenvolvidas internamente podem ser testadas antes de entrarem em produção.

5 CONCLUSÕES

A partir de tudo que foi exposto, pode-se concluir que os testes de detecção de vulnerabilidades são necessários para as instituições financeiras brasileiras, não somente do ponto de vista da conformidade com o disposto por órgão regulador, mas também como ferramenta indispensável para a avaliação do risco de segurança da informação. Os testes oferecem subsídios necessários à detecção de possíveis vulnerabilidades presentes nos sistemas informatizados de uma organização.

Infelizmente, notou-se que mesmo um setor altamente tecnológico como o bancário ainda vê a segurança como burocracia, despesa supérflua ou entrave para avanços na área da tecnologia. É evidente que fragilidades que podem vir a ser exploradas colocam as instituições em uma situação de risco desnecessário, já que existem ferramentas, como os testes de detecção, que podem prevenir futuros ataques. Uma política de gestão de risco bem implantada estabelece processos com grande sucesso na mitigação de riscos, mas muitas empresas parecem alheias a esta realidade. Segundo pesquisa da Associação Brasileira das Entidades dos Mercados Financeiro e de Capitais (ANBIMA, 2018), somente 53 % das instituições financeiras pesquisadas realizaram testes externos de penetração em 2017, apesar de 80 % afirmarem que fazem esse tipo de teste anualmente. Os testes internos foram realizados por apenas 63 % das instituições. Portanto, verificou-se que a mudança necessária é de caráter mais cultural

e, nesse sentido, a imposição regulatória vem como grande aliada, já que força as empresas a estabelecerem uma cultura de segurança de cima para baixo, envolvendo primeiramente o Conselho de Administração e, por conseguinte, todas as outras esferas da organização.

Outra constatação é que, dado o cenário global, com o advento de novas tecnologias e com a crescente informatização bancária, a importância de métodos de avaliação e controle de risco, como os testes de detecção de vulnerabilidades, tende a aumentar ainda mais. Sim, testes exigem tempo e recursos. No entanto, os dados deste artigo demonstram que uma organização que pretende continuar inserida em um mercado que exige completa confiança dos clientes em seus produtos e serviços deve se valer de todas as ferramentas disponíveis para entregar uma experiência segura a seus usuários.

Portanto, conclui-se que as instituições financeiras devem incluir, em sua política de segurança, os testes de detecção de vulnerabilidades. E, com o auxílio de práticas de cibersegurança exigidos pelo regulador norte-americano New York State Department of Financial Services, desenvolveu-se aqui um modelo de cronograma de testes de detecção que, além de colocar as instituições financeiras brasileiras em concordância com as normas e regulamentos federais, ainda proporcionará uma diminuição real dos riscos a que seus sistemas informatizados estão expostos.

REFERÊNCIAS

ANBIMA. **1ª Pesquisa ANBIMA de Cibersegurança 2017**. Disponível em: <http://www.anbima.com.br/data/files/BE/56/71/0C/DB5406101703E9F5A8A80AC2/Relat%C3%B3rio-Pesquisa%20ANBIMA%20de%20Ciberseguran%C3%A7a%202017.pdf?utm_source=especial-ciber&utm_medium=relatorio&utm_campaign=ciber>. Acess em 08 dez. 2018.

BACEN. **Institucional**. Disponível em: <https://www.bcb.gov.br/acessoinformacao/legado?url=https:%2F%2Fwww.bcb.gov.br%2Fpre%2FportalCidadao%2Fbcb%2FbcFaz.asp%3Fidpai%3DLAIINSTITUCIONAL>. Acesso em: 05 ago. 2018.

BACEN. **Resolução nº 4.658, de 26 de abril de 2018**. Dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil. Disponível em: <https://www.bcb.gov.br/pre/normativos/busca/downloadNormativo.asp?arquivo=/Lists/Normativos/Attachments/50581/Res_4658_v1_O.pdf>. Acesso em: 05 ago. 2018.

BOUVERET, Antoine. **Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment**. Disponível em: <http://www.imf.org/~/media/Files/Publications/WP/2018/wp18143.ashx>. Acesso em: 05 ago. 2018.

DELOITTE. **Pesquisa FEBRABAN de Tecnologia Bancária 2018**. Disponível em: <https://cmsportal.febraban.org.br/Arquivos/documentos/PDF/febraban_2018_Final.pdf>. Acesso em 11 dez. 2018.

KIM, David; Solomon, Michael G. **Fundamentos de Segurança de Sistemas de Informação**. Rio de Janeiro: LTC, 2014.

New York State Department of Financial Services. **Cybersecurity Requirements for Financial Services Companies**. Disponível em: <https://www.dfs.ny.gov/legal/regulations/adoptions/dfsrf500txt.pdf>. Acesso em 11 dez. 2018.

NIST. **Guide for Conducting Risk Assessments**. Disponível em: <https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-30r1.pdf>. Acesso em: 05 ago. 2018.

HENRY, Kevin M. **Penetration Testing: Protecting Networks and Systems**. Cambridgeshire: IT Governance Publishing, 2012.

JAGARDE, Christine. **Estimação do Risco Cibernético no Setor Financeiro**. Disponível em: <https://www.imf.org/pt/News/Articles/2018/06/22/blog-estimating-cyber-risk-for-the-financial-sector>. Acesso em: 05 ago. 2018.

ISO 31000 (2018). **Risk Management: Guidelines**. Disponível em: < https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:en>. Acesso em: 08 ago. 2018.

Symantec Corporation. **2017 Norton Cyber Security Insights Report - Global Results**. Disponível em: <http://now.symassets.com/content/dam/norton/global/pdfs/norton_cybersecurity_insights/NCSIR-global-results-US.pdf>. Acesso em 10 dez. 2018.